

30.07.2004

日 本 国 特 許 庁
JAPAN PATENT OFFICE

REC'D 16 SEP 2004

WIPO

PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日 2 0 0 3 年 8 月 5 日
Date of Application:

出 願 番 号 特 願 2 0 0 3 - 2 8 6 6 5 7
Application Number:
[ST. 10/C]: [J P 2 0 0 3 - 2 8 6 6 5 7]

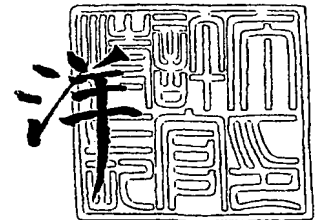
出 願 人 松下電器産業株式会社
Applicant(s):

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH
RULE 17.1(a) OR (b)

2 0 0 4 年 9 月 3 日

特許庁長官
Commissioner,
Japan Patent Office

小 川



BEST AVAILABLE COPY

出証番号 出証特 2 0 0 4 - 3 0 7 9 1 2 5

【書類名】 特許願
【整理番号】 2130050347
【提出日】 平成15年 8月 5日
【あて先】 特許庁長官殿
【国際特許分類】 G09C 1/00
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 山本 直紀
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 石原 秀志
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 館林 誠
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 中野 稔久
【特許出願人】
 【識別番号】 000005821
 【氏名又は名称】 松下電器産業株式会社
【代理人】
 【識別番号】 100097445
 【弁理士】
 【氏名又は名称】 岩橋 文雄
【選任した代理人】
 【識別番号】 100103355
 【弁理士】
 【氏名又は名称】 坂口 智康
【選任した代理人】
 【識別番号】 100109667
 【弁理士】
 【氏名又は名称】 内藤 浩樹
【手数料の表示】
 【予納台帳番号】 011305
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9809938

【書類名】 特許請求の範囲**【請求項 1】**

コンテンツを暗号化して記録する記録装置と、前記暗号化コンテンツを記録する記録媒体と、前記記録媒体に記録された前記暗号化コンテンツを読み出して復号する再生装置とからなる著作権保護システムであって、

前記再生装置はN個（Nは2以上の自然数）のカテゴリに分類されており、

前記記録装置は、メディア鍵と前記N個の各カテゴリに属する再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データを前記N個の各カテゴリに対してそれぞれ生成し、前記メディア鍵に基づいて前記コンテンツを暗号化した暗号化コンテンツを生成し、前記N個の無効化データと前記暗号化コンテンツを前記記録媒体に記録し、

前記再生装置は、前記記録媒体から前記N個の無効化データのうち、前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出し、読み出した前記無効化データに基づいて前記暗号化コンテンツを復号することを特徴とする著作権保護システム。

【請求項 2】

前記N個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであり、

前記各カテゴリの再生装置は、前記記録媒体から対応する前記暗号化メディア鍵データ及び前記暗号化コンテンツを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記メディア鍵を取得し、取得した前記メディア鍵に基づいて前記暗号化コンテンツを復号しすることを特徴とする請求項1記載の著作権保護システム。

【請求項 3】

前記記録装置は、前記メディア鍵に基づいて暗号化鍵を生成し、前記暗号化鍵に基づいて前記コンテンツを暗号化し、

前記各カテゴリの再生装置は、取得した前記メディア鍵に基づいて復号鍵を生成し、生成した前記復号鍵に基づいて前記暗号化コンテンツを復号することを特徴とする請求項2記載の著作権保護システム。

【請求項 4】

前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記メディア鍵で前記コンテンツ鍵を暗号化して暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツ鍵を前記記録媒体に記録し、

前記各カテゴリの再生装置は、前記記録媒体から前記暗号化コンテンツ鍵を読み出し、前記メディア鍵で前記暗号化コンテンツ鍵を復号してコンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号することを特徴とする請求項2記載の著作権保護システム。

【請求項 5】

前記N個の各無効化データは対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、

前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記コンテンツ鍵を前記N個のメディア鍵で暗号化してN個の暗号化コンテンツ鍵を生成し、前記N個の暗号化メディア鍵データと前記N個の暗号化コンテンツ鍵と前記暗号化コンテンツを記録媒体に記録し、

前記各カテゴリの再生装置は、前記記録媒体から対応するカテゴリ用の暗号化メディア鍵データと対応するカテゴリ用の暗号化コンテンツ鍵と前記暗号化コンテンツとを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記対応するカテゴリ用のメディア鍵を取得し、取得した前記対応するカテゴリ用のメディア鍵で前記対応するカテゴリ用の暗号化コンテンツ鍵を復号して前記コンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号することを特徴とする請求項1記載の著作権保護システム。

【請求項 6】

コンテンツに暗号化処理を施して記録する記録装置と、前記暗号化コンテンツを記録する記録媒体と、前記記録媒体に記録された前記暗号化コンテンツを読み出して復号する第2のカテゴリの再生装置と、前記記録媒体に記録された前記暗号化コンテンツを読み出して複合処理の一部を行う前記第2のカテゴリの読み出し装置及び前記第2のカテゴリの読み出し装置に接続され前記暗号化コンテンツの複合処理の一部を行う第1のカテゴリの復号装置とから構成される再生装置とからなる著作権保護システムであって、

前記記録装置は、メディア鍵と前記第1のカテゴリの復号装置が保有するデバイス鍵データとから前記第1のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第1の無効化データを生成し、前記メディア鍵と前記第2のカテゴリの装置が保有するデバイス鍵データとから前記第2のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第2の無効化データを生成し、前記メディア鍵に基づいて前記コンテンツに暗号化処理を施した暗号化コンテンツを生成し、前記第1の無効化データ、前記第2の無効化データ及び前記暗号化コンテンツを前記記録媒体に記録し、

前記第2のカテゴリの再生装置は、前記記録媒体から前記第2の無効化データ及び前記暗号化コンテンツを読み出し、前記第2の無効化データに基づいて前記暗号化コンテンツを復号し、

前記第2のカテゴリの読み出し装置は、前記記録媒体から前記第1の無効化データ、前記第2の無効化データ及び前記暗号化コンテンツを読み出し、前記第2の無効化データに基づいて前記暗号化コンテンツの復号処理の一部を施した中間データ及び前記第1の無効化データを前記第1カテゴリの復号装置に供給し、

前記第1のカテゴリの復号装置は、前記第2のカテゴリの読み出し装置から供給される前記中間データに前記第1の無効化データに基づいて復号処理を施し前記コンテンツを取得することを特徴とする著作権保護システム。

【請求項 7】

コンテンツを暗号化して記録する記録装置であって、

前記記録装置は、メディア鍵とN個（Nは2以上の自然数）のカテゴリに分類された各カテゴリに属する再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データを前記N個の各カテゴリに対してそれぞれ生成し、前記メディア鍵に基づいて前記コンテンツを暗号化した暗号化コンテンツを生成し、前記N個の無効化データと前記暗号化コンテンツを前記記録媒体に記録することを特徴とする記録装置。

【請求項 8】

前記N個の各無効化データは対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであることを特徴とする請求項7記載の記録装置。

【請求項 9】

前記記録装置は、前記メディア鍵に基づいて暗号化鍵を生成し、前記暗号化鍵に基づいて前記コンテンツを暗号化することを特徴とする請求項8記載の記録装置。

【請求項 10】

前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記メディア鍵で前記コンテンツ鍵を暗号化した暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツ鍵を前記記録媒体に記録することを特徴とする請求項8記載の記録装置。

【請求項 11】

前記N個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、

前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記コンテンツ鍵を前記N個のメディア鍵で暗号化してN個の暗号化コンテンツ鍵データを生成し、前記N個の暗号化メディア鍵データと前記N個の暗号化コンテンツ鍵と前記暗号化コンテンツを記録媒体に記録することを特徴とする請求項7記載の記録装置。

【請求項 12】

コンテンツを暗号化して記録する記録装置であって、

前記記録装置は、メディア鍵と第1のカテゴリの復号装置が保有するデバイス鍵データとから前記第1のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第1の無効化データを生成し、前記メディア鍵と前記第2のカテゴリの装置が保有するデバイス鍵データとから前記第2のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第2の無効化データを生成し、前記メディア鍵に基づいて前記コンテンツに暗号化処理を施した暗号化コンテンツを生成し、前記第1の無効化データ、前記第2の無効化データ及び前記暗号化コンテンツを前記記録媒体に記録することを特徴とする記録装置。

【請求項 13】

暗号化コンテンツを記録する記録媒体であって、

前記記録媒体は、メディア鍵とN個（Nは2以上の自然数）のカテゴリに分類された各カテゴリの再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データと、前記メディア鍵に基づいてコンテンツを暗号化して生成された暗号化コンテンツを記録することを特徴とする記録媒体。

【請求項 14】

前記N個の無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであることを特徴とする請求項13記載の記録媒体。

【請求項 15】

前記暗号化コンテンツは、前記メディア鍵に基づいて生成された暗号化鍵に基づいて前記コンテンツを暗号化して生成されたものであることを特徴とする請求項14記載の記録媒体。

【請求項 16】

前記暗号化コンテンツはコンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、

前記メディア鍵で前記コンテンツ鍵を暗号化して生成された暗号化コンテンツ鍵を記録することを特徴とする請求項14記載の記録媒体。

【請求項 17】

前記N個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、

前記暗号化コンテンツは、コンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、

前記記録媒体は、前記コンテンツ鍵を前記N個のメディア鍵で暗号化して生成されたN個の暗号化コンテンツ鍵を記録することを特徴とする請求項13記載の記録媒体。

【請求項 18】

暗号化コンテンツを記録する記録媒体であって、

メディア鍵と第1のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第1のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第1の無効化データと、前記メディア鍵と第2のカテゴリの装置が保有するデバイス鍵データとから生成された前記第2のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第2の無効化データと、前記メディア鍵に基づいて前記コンテンツに暗号化処理を施して生成された暗号化コンテンツとを記録することを特徴とする記録媒体。

【請求項 19】

記録媒体に記録された暗号化コンテンツを再生する再生装置であって、

前記再生装置はN個（Nは2以上の自然数）のカテゴリに分類されており、

前記記録媒体には、メディア鍵と前記N個の各カテゴリの再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データと、前記メディア鍵に基づいてコンテンツを暗号化して生成さ

れた暗号化コンテンツとが記録されており、

前記再生装置は、前記記録媒体から前記N個の無効化データのうち前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出し、読み出した前記無効化データに基づいて前記暗号化コンテンツを復号することを特徴とする再生装置。

【請求項 20】

前記N個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであり、

前記再生装置は、前記記録媒体から対応する前記暗号化メディア鍵データ及び前記暗号化コンテンツを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記メディア鍵を取得し、取得した前記メディア鍵に基づいて前記暗号化コンテンツを復号することを特徴とする請求項 19 記載の再生装置。

【請求項 21】

前記暗号化コンテンツは、前記メディア鍵に基づいて生成された暗号化鍵に基づいて前記コンテンツを暗号化して生成されたものであり、

前記再生装置は、取得した前記メディア鍵に基づいて復号鍵を生成し、生成した前記復号鍵に基づいて前記暗号化コンテンツを復号することを特徴とする請求項 20 記載の再生装置。

【請求項 22】

前記暗号化コンテンツは、コンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、

前記記録媒体には、前記メディア鍵で前記コンテンツ鍵を暗号化して生成された暗号化コンテンツ鍵が記録されており、

前記再生装置は、前記記録媒体から前記暗号化コンテンツ鍵を読み出し、前記メディア鍵で前記暗号化コンテンツ鍵を復号してコンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号することを特徴とする請求項 20 記載の再生装置。

【請求項 23】

前記N個の無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、

前記暗号化コンテンツは、コンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、

前記記録媒体には、前記コンテンツ鍵を前記N個のメディア鍵で暗号化して生成されたN個の暗号化コンテンツ鍵が記録されており、

前記再生装置は、前記記録媒体から対応するカテゴリ用の暗号化メディア鍵データと対応するカテゴリ用の暗号化コンテンツ鍵と前記暗号化コンテンツとを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記対応するカテゴリ用のメディア鍵を取得し、取得した前記対応するカテゴリ用のメディア鍵で前記暗号化コンテンツ鍵を復号して前記コンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号することを特徴とする請求項 19 記載の再生装置。

【請求項 24】

記録媒体に記録された暗号化コンテンツを再生する再生装置であって、

前記記録媒体には、メディア鍵と第1のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第1のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第1の無効化データと、前記メディア鍵と第2のカテゴリの装置が保有するデバイス鍵データとから生成された前記第2のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第2の無効化データと、前記メディア鍵に基づいて暗号化処理を施して生成された暗号化コンテンツとが記録されており、

前記再生装置は、前記第2のカテゴリに属し、前記記録媒体から前記第2の無効化データ及び前記暗号化コンテンツを読み出し、前記第2の無効化データに基づいて前記暗号化コンテンツを復号することを特徴とする再生装置。

【請求項 25】

記録媒体に記録された暗号化コンテンツを再生する再生装置を構成する読み出し装置であって、

前記記録媒体には、メディア鍵と第1のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第1のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第1の無効化データと、前記メディア鍵と第2のカテゴリの装置が保有するデバイス鍵データとから生成された前記第2のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第2の無効化データと、前記メディア鍵に基づいて暗号化処理を施して生成された暗号化コンテンツとが記録されており、

前記読み出し装置は、前記第2のカテゴリに属し、前記記録媒体から前記第1の無効化データ、前記第2の無効化データ及び前記暗号化コンテンツを読み出し、前記第2の無効化データに基づいて前記暗号化コンテンツの復号処理の一部を施した中間データを生成し、生成した前記中間データ及び前記第1の無効化データを出力することを特徴とする読み出し装置。

【請求項 26】

記録媒体に記録された暗号化コンテンツを再生する再生装置を構成する復号装置であって、

前記記録媒体には、メディア鍵と第1のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第1のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第1の無効化データと、前記メディア鍵と第2のカテゴリの装置が保有するデバイス鍵データとから生成された前記第2のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第2の無効化データと、前記メディア鍵に基づいて暗号化処理を施して生成された暗号化コンテンツとが記録されており、

前記第2のカテゴリの読み出し装置は、前記記録媒体から前記第1の無効化データ、前記第2の無効化データ及び前記暗号化コンテンツを読み出し、前記第2の無効化データに基づいて前記暗号化コンテンツの復号処理の一部を施した中間データを生成し、生成した前記中間データ及び前記第1の無効化データを出力し、

前記復号装置は、前記第1のカテゴリに属し、前記第2のカテゴリの読み出し装置から供給される前記中間データに前記第1の無効化データに基づいて復号処理を施して前記コンテンツを取得することを特徴とする復号装置。

【請求項 27】

記録媒体に記録された暗号化コンテンツを再生する再生装置であって、

請求項 25 記載の読み取り装置と請求項 26 記載の復号装置とから構成されることを特徴とする再生装置。

【請求項 28】

コンテンツを暗号化及び復号するために必要な無効化データを生成して記録する鍵生成装置と、コンテンツを暗号化して記録する記録装置と、前記無効化データと前記暗号化コンテンツを記録する記録媒体と、前記記録媒体に記録された前記暗号化コンテンツを読み出して復号する再生装置とからなる著作権保護システムであって、

前記記録装置及び前記再生装置はN個（Nは2以上の自然数）のカテゴリに分類されており、

前記鍵生成装置は、メディア鍵と前記各カテゴリに属する記録装置もしくは再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の記録装置もしくは再生装置が保有するデバイス鍵を無効化するための無効化データを、前記N個の各カテゴリに対してそれぞれ生成し、生成した前記N個の無効化データを前記記録媒体に記録し、

前記記録装置は、前記記録媒体から前記N個の無効化データのうち、前記記録装置が属するカテゴリ用の無効化データを読み出し、読み出した前記無効化データに基づいてコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを前記記録媒体に記録し、

前記再生装置は、前記記録媒体から前記N個の無効化データのうち、前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出し、読み出した前記無

効化データに基づいて前記暗号化コンテンツを復号することを特徴とする著作権保護システム。

【請求項 29】

メディア鍵とN個（Nは2以上の自然数）のカテゴリに分類された各カテゴリに属する記録装置もしくは再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の記録装置もしくは再生装置が保有するデバイス鍵を無効化するための無効化データを、前記N個の各カテゴリに対してそれぞれ生成し、生成した前記N個の無効化データを前記記録媒体に記録することを特徴とする鍵生成装置。

【請求項 30】

コンテンツを暗号化して記録する記録装置であって、

メディア鍵とN個（Nは2以上の自然数）のカテゴリに分類された各カテゴリに属する記録装置もしくは再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の記録装置もしくは再生装置が保有するデバイス鍵を無効化するための無効化データが記録された記録媒体から、前記N個の無効化データのうち前記記録装置が属するカテゴリ用の無効化データを読み出し、

読み出した前記無効化データに基づいてコンテンツを暗号化して暗号化コンテンツを生成し、

生成した前記暗号化コンテンツを前記記録媒体に記録することを特徴とする記録装置。

【書類名】明細書

【発明の名称】著作権保護システム、鍵生成装置、記録装置、再生装置、読み出し装置、復号装置、及び記録媒体

【技術分野】

【0001】

本発明は、映画や音楽などの著作物をデジタル化したコンテンツを、光ディスク等の大容量記録媒体に記録して、再生するシステムに関し、特にコンテンツの著作権者の許可なく不正利用されることを防止する著作権保護システムに関する。

【背景技術】

【0002】

近年、記録媒体が大容量化するに従い、映画や音楽などの著作物をデジタル化したコンテンツを例えば光ディスク等の記録媒体に格納して市販するビジネスが盛んに行われている。

【0003】

記録媒体に記録されたコンテンツは、不正にコピーされる可能性があるため、何らかの保護が必要である。

【0004】

一般的に、コンテンツの著作権を保護するため、即ちコンテンツの不正再生や不正コピー等といった不正利用を防止するために暗号化技術が用いられる。

【0005】

具体的には、コンテンツをある暗号化鍵を用いて暗号化して光ディスク等の記録媒体に記録して配布する。これに対して、その暗号鍵に対応する復号鍵を保有する端末のみが、記録媒体から読み出したデータをその復号鍵を用いて復号し、コンテンツの再生等を行うことができる。

【0006】

なお、コンテンツを暗号化して記録媒体に記録する方法としては、端末が保有する復号鍵に対応する暗号化鍵でコンテンツそのものを暗号化して記録する方法や、コンテンツをある鍵で暗号化して記録した上で、その鍵に対応する復号用の鍵を、端末が保有する復号鍵に対応する暗号化鍵で暗号化して記録する方法とがある。

【0007】

このとき、端末が保有する復号鍵は外部に露見しないように厳重に管理される必要があるが、不正者による端末内部の解析によって、ある鍵が外部に暴露される危険性がある。ある鍵が一旦不正者に暴露されてしまうと、コンテンツを不正利用する再生装置あるいはソフトウェアを作成し、インターネット等によりそれらを流布することが考えられる。このような場合、著作権者は一旦暴露された鍵では、次から提供するコンテンツを扱えないようにしたいと考える。これを実現する技術を鍵無効化技術と呼び、鍵無効化を実現するシステムとして、特許文献1が開示されている。

【0008】

一方、記録媒体に記録された暗号化コンテンツを再生する装置としては、記録媒体から暗号化コンテンツを読み出す機能と読み出した暗号化コンテンツを復号する機能が一体となったいわゆる民生用プレーヤや、パソコンに接続もしくは内蔵された光ディスクドライブで記録媒体から暗号化コンテンツを読み出し、読み出した暗号化コンテンツをパソコンのホスト上で動作するアプリケーションプログラムによって復号して再生するものがある。これら2つの種類の再生装置に対応する著作権保護システムとして、非特許文献1が開示されている。

【特許文献1】特開2002-281013号公報

【非特許文献1】Content Protection for Pre-recorded Media DVD Book, 4C Entity, LLC

【発明の開示】

【発明が解決しようとする課題】

【0009】

しかしながら、上記したような従来の著作権保護システムでは、対象とするすべての種類の再生装置に対して共通の無効化データを記録媒体に記録するようにしているため、各再生装置はその無効化データ全体を記録媒体から読み込んで少なくとも一時的に格納するメモリを装置内に設ける必要がある。

【0010】

また、一般に民生用プレーヤにおいては、装置に組み込まれた処理アルゴリズムや鍵の長さを変更することは、時間と手間がかかり困難である。一方、パソコン上のアプリケーションプログラムとして復号処理や鍵がソフトウェアで実装される場合は、一般的にハードウェアで実装する場合に比べて、内蔵する復号アルゴリズムや鍵の更新や追加は容易であるが、復号アルゴリズムや鍵の堅牢な実装は困難である。しかしながら、従来の共通の無効化データを記録媒体に記録する著作権保護システムでは、パソコンのホスト上で動作するアプリケーションプログラムが不正に解析されてアルゴリズムや多数の鍵が暴露された場合であっても、暗号化・復号のアルゴリズムや鍵長を変更することは実質上不可能となっている。これは、無効化機能が正しく働かなくなることを意味し、不正機器によりコンテンツの不正利用が蔓延することにつながる。

【0011】

本発明では、上記課題を解決するために、再生装置内に設けるメモリのサイズを小さくでき、かつ、パソコンのホスト上で動作するアプリケーションプログラムが不正に解析されてアルゴリズムや多数の鍵が暴露された場合でも、暗号化・復号のアルゴリズムや鍵長を変更することでシステム全体の無効化機能を維持することのできる著作権保護システムを提供する。

【課題を解決するための手段】**【0012】**

本発明は、コンテンツを暗号化して記録する記録装置と、前記暗号化コンテンツを記録する記録媒体と、前記記録媒体に記録された前記暗号化コンテンツを読み出して復号する再生装置とからなる著作権保護システムであって、前記再生装置はN個（Nは2以上の自然数）のカテゴリに分類されており、前記記録装置は、メディア鍵と前記N個の各カテゴリに属する再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データを前記N個の各カテゴリに対してそれぞれ生成し、前記メディア鍵に基づいて前記コンテンツを暗号化した暗号化コンテンツを生成し、前記N個の無効化データと前記暗号化コンテンツを前記記録媒体に記録し、前記再生装置は、前記記録媒体から前記N個の無効化データのうち、前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出し、読み出した前記無効化データに基づいて前記暗号化コンテンツを復号することを特徴とする。

【0013】

また、本発明は、前記著作権保護システムであって、前記N個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであり、前記各カテゴリの再生装置は、前記記録媒体から対応する前記暗号化メディア鍵データ及び前記暗号化コンテンツを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記メディア鍵を取得し、取得した前記メディア鍵に基づいて前記暗号化コンテンツを復号しすることを特徴とする。

【0014】

また、本発明は、前記著作権保護システムであって、前記記録装置は、前記メディア鍵に基づいて暗号化鍵を生成し、前記暗号化鍵に基づいて前記コンテンツを暗号化し、前記各カテゴリの再生装置は、取得した前記メディア鍵に基づいて復号鍵を生成し、生成した前記復号鍵に基づいて前記暗号化コンテンツを復号することを特徴とする。

【0015】

また、本発明は、前記著作権保護システムであって、前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記メディア鍵で前記コンテンツ鍵を暗号化して暗号化コン

テンツ鍵を生成し、生成した前記暗号化コンテンツ鍵を前記記録媒体に記録し、前記各カテゴリの再生装置は、前記記録媒体から前記暗号化コンテンツ鍵を読み出し、前記メディア鍵で前記暗号化コンテンツ鍵を復号してコンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号することを特徴とする。

【0016】

また、本発明は、前記著作権保護システムであって、前記N個の各無効化データは対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記コンテンツ鍵を前記N個のメディア鍵で暗号化してN個の暗号化コンテンツ鍵を生成し、前記N個の暗号化メディア鍵データと前記N個の暗号化コンテンツ鍵と前記暗号化コンテンツを記録媒体に記録し、前記各カテゴリの再生装置は、前記記録媒体から対応するカテゴリ用の暗号化メディア鍵データと対応するカテゴリ用の暗号化コンテンツ鍵と前記暗号化コンテンツとを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記対応するカテゴリ用のメディア鍵を取得し、取得した前記対応するカテゴリ用のメディア鍵で前記対応するカテゴリ用の暗号化コンテンツ鍵を復号して前記コンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号することを特徴とする。

【0017】

また、本発明は、コンテンツに暗号化処理を施して記録する記録装置と、前記暗号化コンテンツを記録する記録媒体と、前記記録媒体に記録された前記暗号化コンテンツを読み出して復号する第2のカテゴリの再生装置と、前記記録媒体に記録された前記暗号化コンテンツを読み出して複合処理の一部を行う前記第2のカテゴリの読み出し装置及び前記第2のカテゴリの読み出し装置に接続され前記暗号化コンテンツの複合処理の一部を行う第1のカテゴリの復号装置とから構成される再生装置とからなる著作権保護システムであって、前記記録装置は、メディア鍵と前記第1のカテゴリの復号装置が保有するデバイス鍵データとから前記第1のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第1の無効化データを生成し、前記メディア鍵と前記第2のカテゴリの装置が保有するデバイス鍵データとから前記第2のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第2の無効化データを生成し、前記メディア鍵に基づいて前記コンテンツに暗号化処理を施した暗号化コンテンツを生成し、前記第1の無効化データ、前記第2の無効化データ及び前記暗号化コンテンツを前記記録媒体に記録し、前記第2のカテゴリの再生装置は、前記記録媒体から前記第2の無効化データ及び前記暗号化コンテンツを読み出し、前記第2の無効化データに基づいて前記暗号化コンテンツを復号し、前記第2のカテゴリの読み出し装置は、前記記録媒体から前記第1の無効化データ、前記第2の無効化データ及び前記暗号化コンテンツを読み出し、前記第2の無効化データに基づいて前記暗号化コンテンツの復号処理の一部を施した中間データ及び前記第1の無効化データを前記第1カテゴリの復号装置に供給し、前記第1のカテゴリの復号装置は、前記第2のカテゴリの読み出し装置から供給される前記中間データに前記第1の無効化データに基づいて復号処理を施し前記コンテンツを取得することを特徴とする。

【0018】

また、本発明は、コンテンツを暗号化して記録する記録装置であって、メディア鍵とN個（Nは2以上の自然数）のカテゴリに分類された各カテゴリに属する再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データを前記N個の各カテゴリに対してそれぞれ生成し、前記メディア鍵に基づいて前記コンテンツを暗号化した暗号化コンテンツを生成し、前記N個の無効化データと前記暗号化コンテンツを前記記録媒体に記録することを特徴とする。

【0019】

また、本発明は、前記記録装置であって、前記N個の各無効化データは対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであることを特徴とする。

【0020】

また、本発明は、前記記録装置であって、前記メディア鍵に基づいて暗号化鍵を生成し、前記暗号化鍵に基づいて前記コンテンツを暗号化することを特徴とする。

【0021】

また、本発明は、前記記録装置であって、コンテンツ鍵で前記コンテンツを暗号化し、前記メディア鍵で前記コンテンツ鍵を暗号化した暗号化コンテンツ鍵を生成し、生成した前記暗号化コンテンツ鍵を前記記録媒体に記録することを特徴とする。

【0022】

また、本発明は、前記記録装置であって、前記N個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、前記記録装置は、コンテンツ鍵で前記コンテンツを暗号化し、前記コンテンツ鍵を前記N個のメディア鍵で暗号化してN個の暗号化コンテンツ鍵データを生成し、前記N個の暗号化メディア鍵データと前記N個の暗号化コンテンツ鍵と前記暗号化コンテンツを記録媒体に記録することを特徴とする。

【0023】

また、本発明は、コンテンツを暗号化して記録する記録装置であって、メディア鍵と第1のカテゴリの復号装置が保有するデバイス鍵データとから前記第1のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第1の無効化データを生成し、前記メディア鍵と前記第2のカテゴリの装置が保有するデバイス鍵データとから前記第2のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第2の無効化データを生成し、前記メディア鍵に基づいて前記コンテンツに暗号化処理を施した暗号化コンテンツを生成し、前記第1の無効化データ、前記第2の無効化データ及び前記暗号化コンテンツを前記記録媒体に記録することを特徴とする。

【0024】

また、本発明は、暗号化コンテンツを記録する記録媒体であって、メディア鍵とN個（Nは2以上の自然数）のカテゴリに分類された各カテゴリの再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データと、前記メディア鍵に基づいてコンテンツを暗号化して生成された暗号化コンテンツを記録することを特徴とする。

【0025】

また、本発明は、前記記録媒体であって、前記N個の無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであることを特徴とする。

【0026】

また、本発明は、前記記録媒体であって、前記暗号化コンテンツは、前記メディア鍵に基づいて生成された暗号化鍵に基づいて前記コンテンツを暗号化して生成されたものであることを特徴とする。

【0027】

また、本発明は、前記記録媒体であって、前記暗号化コンテンツはコンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、前記メディア鍵で前記コンテンツ鍵を暗号化して生成された暗号化コンテンツ鍵を記録することを特徴とする。

【0028】

また、本発明は、前記記録媒体であって、前記N個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、前記暗号化コンテンツは、コンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、前記記録媒体は、前記コンテンツ鍵を前記N個のメディア鍵で暗号化して生成されたN個の暗号化コンテンツ鍵を記録することを特徴とする。

【0029】

また、本発明は、暗号化コンテンツを記録する記録媒体であって、メディア鍵と第1の

カテゴリの復号装置が保有するデバイス鍵データとから生成された前記第1のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第1の無効化データと、前記メディア鍵と第2のカテゴリの装置が保有するデバイス鍵データとから生成された前記第2のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第2の無効化データと、前記メディア鍵に基づいて前記コンテンツに暗号化処理を施して生成された暗号化コンテンツとを記録することを特徴とする。

【0030】

また、本発明は、記録媒体に記録された暗号化コンテンツを再生する再生装置であって、前記再生装置はN個（Nは2以上の自然数）のカテゴリに分類されており、前記記録媒体には、メディア鍵と前記N個の各カテゴリの再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の再生装置が保有するデバイス鍵を無効化するための無効化データと、前記メディア鍵に基づいてコンテンツを暗号化して生成された暗号化コンテンツとが記録されており、前記再生装置は、前記記録媒体から前記N個の無効化データのうち前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出し、読み出した前記無効化データに基づいて前記暗号化コンテンツを復号することを特徴とする。

【0031】

また、本発明は、前記再生装置であって、前記N個の各無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記メディア鍵を暗号化した暗号化メディア鍵データであり、前記再生装置は、前記記録媒体から対応する前記暗号化メディア鍵データ及び前記暗号化コンテンツを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記メディア鍵を取得し、取得した前記メディア鍵に基づいて前記暗号化コンテンツを復号することを特徴とする。

【0032】

また、本発明は、前記再生装置であって、前記暗号化コンテンツは、前記メディア鍵に基づいて生成された暗号化鍵に基づいて前記コンテンツを暗号化して生成されたものであり、前記再生装置は、取得した前記メディア鍵に基づいて復号鍵を生成し、生成した前記復号鍵に基づいて前記暗号化コンテンツを復号することを特徴とする。

【0033】

また、本発明は、前記再生装置であって、前記暗号化コンテンツは、コンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、前記記録媒体には、前記メディア鍵で前記コンテンツ鍵を暗号化して生成された暗号化コンテンツ鍵が記録されており、前記再生装置は、前記記録媒体から前記暗号化コンテンツ鍵を読み出し、前記メディア鍵で前記暗号化コンテンツ鍵を復号してコンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号することを特徴とする。

【0034】

また、本発明は、前記再生装置であって、前記N個の無効化データは、対応するカテゴリの再生装置が保有するデバイス鍵データで前記対応するカテゴリ用のメディア鍵を暗号化した暗号化メディア鍵データであり、前記暗号化コンテンツは、コンテンツ鍵で前記コンテンツを暗号化して生成されたものであり、前記記録媒体には、前記コンテンツ鍵を前記N個のメディア鍵で暗号化して生成されたN個の暗号化コンテンツ鍵が記録されており、前記再生装置は、前記記録媒体から対応するカテゴリ用の暗号化メディア鍵データと対応するカテゴリ用の暗号化コンテンツ鍵と前記暗号化コンテンツとを読み出し、保有するデバイス鍵で前記暗号化メディア鍵データを復号して前記対応するカテゴリ用のメディア鍵を取得し、取得した前記対応するカテゴリ用のメディア鍵で前記暗号化コンテンツ鍵を復号して前記コンテンツ鍵を取得し、取得した前記コンテンツ鍵で前記暗号化コンテンツを復号することを特徴とする。

【0035】

また、本発明は、記録媒体に記録された暗号化コンテンツを再生する再生装置であって、前記記録媒体には、メディア鍵と第1のカテゴリの復号装置が保有するデバイス鍵デー

タとから生成された前記第1のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第1の無効化データと、前記メディア鍵と第2のカテゴリの装置が保有するデバイス鍵データとから生成された前記第2のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第2の無効化データと、前記メディア鍵に基づいて暗号化処理を施して生成された暗号化コンテンツとが記録されており、前記再生装置は、前記第2のカテゴリに属し、前記記録媒体から前記第2の無効化データ及び前記暗号化コンテンツを読み出し、前記第2の無効化データに基づいて前記暗号化コンテンツを復号することを特徴とする。

【0036】

また、本発明は、記録媒体に記録された暗号化コンテンツを再生する再生装置を構成する読み出し装置であって、前記記録媒体には、メディア鍵と第1のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第1のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第1の無効化データと、前記メディア鍵と第2のカテゴリの装置が保有するデバイス鍵データとから生成された前記第2のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第2の無効化データと、前記メディア鍵に基づいて暗号化処理を施して生成された暗号化コンテンツとが記録されており、前記読み出し装置は、前記第2のカテゴリに属し、前記記録媒体から前記第1の無効化データ、前記第2の無効化データ及び前記暗号化コンテンツを読み出し、前記第2の無効化データに基づいて前記暗号化コンテンツの復号処理の一部を施した中間データを生成し、生成した前記中間データ及び前記第1の無効化データを出力することを特徴とする。

【0037】

また、本発明は、記録媒体に記録された暗号化コンテンツを再生する再生装置を構成する復号装置であって、前記記録媒体には、メディア鍵と第1のカテゴリの復号装置が保有するデバイス鍵データとから生成された前記第1のカテゴリの特定の復号装置が保有するデバイス鍵を無効化するための第1の無効化データと、前記メディア鍵と第2のカテゴリの装置が保有するデバイス鍵データとから生成された前記第2のカテゴリの特定の装置が保有するデバイス鍵を無効化するための第2の無効化データと、前記メディア鍵に基づいて暗号化処理を施して生成された暗号化コンテンツとが記録されており、前記第2のカテゴリの読み出し装置は、前記記録媒体から前記第1の無効化データ、前記第2の無効化データ及び前記暗号化コンテンツを読み出し、前記第2の無効化データに基づいて前記暗号化コンテンツの復号処理の一部を施した中間データを生成し、生成した前記中間データ及び前記第1の無効化データを出力し、前記復号装置は、前記第1のカテゴリに属し、前記第2のカテゴリの読み出し装置から供給される前記中間データに前記第1の無効化データに基づいて復号処理を施して前記コンテンツを取得することを特徴とする。

【0038】

また、本発明は、記録媒体に記録された暗号化コンテンツを再生する再生装置であって、請求項25記載の読み取り装置と請求項26記載の復号装置とから構成されることを特徴とする。

【0039】

また、本発明は、コンテンツを暗号化及び復号するために必要な無効化データを生成して記録する鍵生成装置と、コンテンツを暗号化して記録する記録装置と、前記無効化データと前記暗号化コンテンツを記録する記録媒体と、前記記録媒体に記録された前記暗号化コンテンツを読み出して復号する再生装置とからなる著作権保護システムであって、前記記録装置及び前記再生装置はN個（Nは2以上の自然数）のカテゴリに分類されており、前記鍵生成装置は、メディア鍵と前記各カテゴリに属する記録装置もしくは再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の記録装置もしくは再生装置が保有するデバイス鍵を無効化するための無効化データを、前記N個の各カテゴリに対してそれぞれ生成し、生成した前記N個の無効化データを前記記録媒体に記録し、前記記録装置は、前記記録媒体から前記N個の無効化データのうち、前記記録装置が属するカテゴリ用の

無効化データを読み出し、読み出した前記無効化データに基づいてコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを前記記録媒体に記録し、前記再生装置は、前記記録媒体から前記N個の無効化データのうち、前記再生装置が属するカテゴリ用の無効化データ及び前記暗号化コンテンツを読み出し、読み出した前記無効化データに基づいて前記暗号化コンテンツを復号することを特徴とする。

【0040】

また、本発明は、鍵生成装置であって、メディア鍵とN個（Nは2以上の自然数）のカテゴリに分類された各カテゴリに属する記録装置もしくは再生装置が保有するデバイス鍵データとから前記各カテゴリの特定の記録装置もしくは再生装置が保有するデバイス鍵を無効化するための無効化データを、前記N個の各カテゴリに対してそれぞれ生成し、生成した前記N個の無効化データを前記記録媒体に記録することを特徴とする。

【0041】

また、本発明は、コンテンツを暗号化して記録する記録装置であって、メディア鍵とN個（Nは2以上の自然数）のカテゴリに分類された各カテゴリに属する記録装置もしくは再生装置が保有するデバイス鍵データとから生成された前記各カテゴリの特定の記録装置もしくは再生装置が保有するデバイス鍵を無効化するための無効化データが記録された記録媒体から、前記N個の無効化データのうち前記記録装置が属するカテゴリ用の無効化データを読み出し、読み出した前記無効化データに基づいてコンテンツを暗号化して暗号化コンテンツを生成し、生成した前記暗号化コンテンツを前記記録媒体に記録することを特徴とする。

【発明の効果】

【0042】

本発明によれば、第1のカテゴリの装置及び第2のカテゴリの装置は、それぞれ異なるカテゴリの装置を無効化するための第1もしくは第2の暗号化メディア鍵を読み込む必要がないため、装置内に設けるメモリ容量を小さくでき、処理時間も短くできる。また、第1の暗号化メディア鍵の生成に用いる暗号化アルゴリズムを第2の暗号化メディア鍵の生成に用いる暗号化アルゴリズムと異なるものとすることができるため、第1のカテゴリの再生装置の無効化システムが暴露されるような事態に陥った場合にも、第1のカテゴリの再生装置に付与するデバイス鍵の鍵長や第1の暗号化メディア鍵の生成アルゴリズムを変更することで、第2のカテゴリの再生装置に影響を与えることなく、無効化システムを更新することができる。

【発明を実施するための最良の形態】

【0043】

以下、本発明の実施の形態について、図面を参照しながら説明する。

【0044】

（実施の形態1）

本発明の実施の形態1は、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものである。

【0045】

以下、本発明の実施の形態1について、図面を参照しながら説明する。図1は、コンテンツを暗号化して記録する記録装置100及び記録媒体120を示しており、図2は、記録媒体120から暗号化コンテンツを読み出して復号する第1のカテゴリの再生装置200を示しており、図3は、記録媒体120から暗号化コンテンツを読み出して復号する第2のカテゴリの再生装置300を示している。また、図4は記録媒体120に記録される各種データ的具体例を示している。

【0046】

記録装置100は、第1のカテゴリの各再生装置が秘密に保有するデバイス鍵を格納する第1のデバイス鍵格納部101と、第2のカテゴリの各再生装置が秘密に保有するデバイス鍵を格納する第2のデバイス鍵格納部102と、メディア鍵を暗号化するために用いるデバイス鍵を選択する第1のデバイス鍵選択部103及び第2のデバイス鍵選択部10

4と、外部から入力されるメディア鍵を第1のデバイス鍵選択部103で選択したデバイス鍵で暗号化する第1のメディア鍵暗号化部105と、メディア鍵を第2のデバイス鍵選択部104で選択したデバイス鍵で暗号化する第2のメディア鍵暗号化部106と、外部から入力されるコンテンツ鍵をメディア鍵で暗号化するコンテンツ鍵暗号化部107と、同じく外部から入力されるコンテンツを暗号化するコンテンツ暗号化部108とを備える。

【0047】

なお、図1には示していないが、第1のメディア鍵暗号化部105には、第1のカテゴリの再生装置のうち無効化すべき再生装置の情報が、第2のメディア鍵暗号化部106には第2のカテゴリの再生装置のうち無効化すべき再生装置の情報が、それぞれ入力されており、暗号化メディア鍵を生成する際にこれら無効化すべき再生装置では正しいメディア鍵が復号できないように暗号化メディア鍵を生成する。さらにメディア鍵は記録媒体を製造する度に、コンテンツ鍵はコンテンツ毎に異なる鍵データを選択している。

【0048】

記録媒体120は、第1のメディア鍵暗号化部105が生成した第1の暗号化メディア鍵データを記録する第1の暗号化メディア鍵データ記録領域121と、第2のメディア鍵暗号化部106が生成した第2の暗号化メディア鍵データを記録する第2の暗号化メディア鍵データ記録領域122と、コンテンツ鍵暗号化部107が生成した暗号化コンテンツ鍵を記録する暗号化コンテンツ鍵記録領域123と、コンテンツ暗号化部108が生成した暗号化コンテンツを記録する暗号化コンテンツ記録領域124とを備える。

【0049】

第1のカテゴリの再生装置200は、デバイス鍵を秘密に保有するデバイス鍵格納部201と、デバイス鍵を用いて記録媒体120から読み出した第1の暗号化メディア鍵データを復号してメディア鍵を取得するメディア鍵復号部202と、取得したメディア鍵を用いて記録媒体120から読み出した暗号化コンテンツ鍵を復号してコンテンツ鍵を取得するコンテンツ鍵復号部203と、取得したコンテンツ鍵を用いて記録媒体120から読み出した暗号化コンテンツを復号するコンテンツ復号部204とを備える。本実施の形態ではパソコン上のアプリケーションプログラムのようにソフトウェアで実装される再生装置を第1のカテゴリに属する再生装置とした。

【0050】

第2のカテゴリの再生装置300は、デバイス鍵を秘密に保有するデバイス鍵格納部301と、デバイス鍵を用いて記録媒体120から読み出した第2の暗号化メディア鍵データを復号してメディア鍵を取得するメディア鍵復号部302と、取得したメディア鍵を用いて記録媒体120から読み出した暗号化コンテンツ鍵を復号してコンテンツ鍵を取得するコンテンツ鍵復号部303と、取得したコンテンツ鍵を用いて記録媒体120から読み出した暗号化コンテンツを復号するコンテンツ復号部304とを備える。本実施の形態では一般的な民生プレーヤのようにハードウェアで実装される再生装置を第2のカテゴリに属する再生装置とした。

【0051】

図4は、 m 台の第1のカテゴリの再生装置及び n 台の第2のカテゴリの再生装置がそれぞれ固有のデバイス鍵を1個だけ保有しており、第1のカテゴリの再生装置2と第2のカテゴリの再生装置3が無効化されているとした場合の、記録媒体120に記録される各種データの具体例を示している。図4中で、第1のカテゴリの再生装置 i ($i=1\sim m$) が保有するデバイス鍵を DKA_i 、第2のカテゴリの再生装置 j ($j=1\sim n$) が保有するデバイス鍵を DKB_j としている。また、 $E_a(X, Y)$ 、 $E_b(X, Y)$ 、 $E_c(X, Y)$ 及び $E_d(X, Y)$ はデータ Y を鍵データ X を用いて暗号化する関数を意味する。なお、使用される暗号アルゴリズムは、公知の技術で実現可能であり、本実施の形態では鍵長56bitのDES暗号を使用した。

【0052】

(第1の暗号化メディア鍵データ記録領域121)

第1の暗号化メディア鍵データ記録領域121には、第1のカテゴリの再生装置が保有するデバイス鍵(DKA1~DKAm)で暗号化されたメディア鍵(MK)が記録されている。ここで、第1のカテゴリの再生装置2は無効化されており、DKA2ではメディア鍵(MK)とはまったく無関係のデータ「0」が暗号化されて記録されている。これは第1の暗号化メディア鍵を生成する際に、第1のメディア鍵暗号化部105において、第1のカテゴリのうち無効化すべき再生装置の情報として再生装置2が入力され、再生装置2では正しいメディア鍵が得られないように処理された結果である。

【0053】

(第2の暗号化メディア鍵データ記録領域122)

第2の暗号化メディア鍵データ記録領域122には、第2のカテゴリの再生装置が保有するデバイス鍵(DKB1~DKBn)で暗号化されたメディア鍵(MK)が記録されている。ここで、第2のカテゴリの再生装置3は無効化されており、DKB3ではメディア鍵(MK)とはまったく無関係のデータ「0」が暗号化されて記録されている。これは第2の暗号化メディア鍵を生成する際に、第2のメディア鍵暗号化部106において、第2のカテゴリのうち無効化すべき再生装置の情報として再生装置3が入力され、再生装置3では正しいメディア鍵が得られないように処理された結果である。

【0054】

第1及び第2の暗号化メディア鍵データをこのように生成することにより、第1のカテゴリの再生装置2及び第2のカテゴリの再生装置3を除く再生装置が正しいメディア鍵(MK)を復号することができるとともに、第1のカテゴリの再生装置2及び第2のカテゴリの再生装置3をシステムから排除することができる。

【0055】

(暗号化コンテンツ鍵記録領域123)

暗号化コンテンツ鍵記録領域123にはメディア鍵(MK)で暗号化されたコンテンツ鍵(CK)が記録されている。

【0056】

(暗号化コンテンツ記録領域124)

暗号化コンテンツ記録領域124には、コンテンツ鍵(CK)で暗号化されたコンテンツが記録されている。

【0057】

以上のように構成された本発明の実施の形態1において、例えば第1のカテゴリの再生装置に付与したデバイス鍵の多数や、第1の暗号化メディア鍵データを復号するアルゴリズムがインターネット上で不正に公開され、第1のカテゴリの再生装置の無効化が機能しなくなったと判断された場合には、第1のカテゴリの再生装置の無効化システムを更新することになる。以下、その具体例を説明する。

【0058】

(システム更新の具体例1)

第1のカテゴリの再生装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体120に記録する各種データの具体例1を図5に示す。図4との違いは、第1の暗号化メディア鍵データの生成に用いるデバイス鍵をDKA1~DKAmからDKA'1~DKA'mに変更したことである。ここで、新たなデバイス鍵(DKA'1~DKA'm)のうちの各デバイス鍵は、システム更新前のデバイス鍵(DKA1~DKAm)のどれとも一致しないようになっている。

【0059】

一方、無効化されていない第1のカテゴリの再生装置200には、新たなデバイス鍵が付与され、デバイス鍵格納部201に格納される。例えば、第1のカテゴリの再生装置mは、以前から保有していたデバイス鍵(DKAm)に加え、新たに付与されたデバイス鍵(DKA'm)をデバイス鍵格納部201に保有する。再生装置mは、図4の記録媒体を再生する際には、デバイス鍵DKAmを用い、無効化システム更新後の図5の記録媒体を再生する際には、デバイス鍵DKA'mを用いて、記録媒体から読み出した第1の暗号化

メディア鍵を復号してメディア鍵(MK)を取得し、取得したメディア鍵(MK)を用いて暗号化コンテンツ鍵を復号してコンテンツ鍵(CK)を取得し、取得したコンテンツ鍵(CK)を用いて暗号化コンテンツを復号再生する。

【0060】

ここで、新たなデバイス鍵(DKA' 1~DKA' m)のうちの各デバイス鍵は、システム更新前のデバイス鍵(DKA 1~DKA m)のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵がDKA 2以外に存在したとしても、そのデバイス鍵を使って図5の記録媒体から読み出した第1の暗号化メディア鍵を復号してメディア鍵(MK)を取得することはできず、コンテンツを再生することはできない。

【0061】

なお、上記したシステム更新に際して、第2の暗号化メディア鍵データの生成に用いるデバイス鍵(DKB 1~DKB n)は変更されていないので、第2のカテゴリに属する再生装置には何らの変更を加える必要がない。

【0062】

(システム更新の具体例2)

第1のカテゴリの再生装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体120に記録する各種データの具体例2を図6に示す。図4との違いは、第1の暗号化メディア鍵の生成に用いるデバイス鍵をDKA 1~DKA mからDKA' 1~DKA' mに変更したことと、暗号化アルゴリズムをEa(X, Y)からEa'(X, Y)に変更したことである。ここで、新たなデバイス鍵(DKA' 1~DKA' m)のうちの各デバイス鍵は、システム更新前のデバイス鍵(DKA 1~DKA m)のどれとも一致しないようになっている。

【0063】

一方、無効化されていない第1のカテゴリの各再生装置200には、新たなデバイス鍵を付与されデバイス鍵格納部201に格納される。また、メディア鍵復号部202には、以前から組み込まれている図4の第1の暗号化メディア鍵データを復号するための復号アルゴリズムDa(X, Y)に加えて、図5の第1の暗号化メディア鍵データを復号するための復号アルゴリズムDa'(X, Y)が組み込まれる。例えば、第1のカテゴリの再生装置mは、以前から保有していたデバイス鍵(DKA m)に加え、新たに付与されたデバイス鍵(DKA' m)を保有する。再生装置mは、図4の記録媒体を再生する際には、デバイス鍵DKA mと暗号化アルゴリズムDa(X, Y)を用い、図5の記録媒体を再生する際には、デバイス鍵DKA' mと暗号化アルゴリズムDa'(X, Y)を用いて、記録媒体から読み出した第1の暗号化メディア鍵データを復号してメディア鍵(MK)を取得し、取得したメディア鍵(MK)を用いて暗号化コンテンツ鍵を復号してコンテンツ鍵(CK)を取得し、取得したコンテンツ鍵(CK)を用いて暗号化コンテンツを復号する。本実施の形態ではEa(X, Y)及びDa(X, Y)は鍵長56bitのDES暗号を用いたのに対して、Ea'(X, Y)及びDa'(X, Y)では2キートリプルDESと呼ばれる鍵長112bitの暗号を用いた。

【0064】

ここで、新たなデバイス鍵(DKA' 1~DKA' m)のうちの各デバイス鍵は、システム更新前のデバイス鍵(DKA 1~DKA m)のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵がDKA 2以外に存在したとしても、そのデバイス鍵を使って図5の記録媒体から読み出した第1の暗号化メディア鍵データを復号してメディア鍵(MK)を取得することはできず、コンテンツを再生することはできない。

【0065】

また、デバイス鍵の鍵長や暗号アルゴリズムを変更して暗号強度の高いものにすることができ、システムを解析してデバイス鍵を不正取得するといった行為を困難にすることができる。

【0066】

なお、上記したシステム更新に際して、第2の暗号化メディア鍵データの生成に用いるデバイス鍵(DKB1~DKBn)及び第2の暗号化メディア鍵データの暗号化アルゴリズムは変更されていないので、第2のカテゴリに属する再生装置には何らの変更を加える必要がない。

【0067】

なお、システム更新の具体例1、2ともに記録媒体にはシステム更新の世代に関する情報を記録しており、第1のカテゴリの再生装置はこの情報に基づいて、いずれの世代のデバイス鍵あるいはアルゴリズムを使用するかを判断する。

【0068】

以上のように構成された本発明の実施の形態1によれば、第1のカテゴリの再生装置200及び第2のカテゴリの再生装置300は、それぞれ異なるカテゴリの再生装置を無効化するための第1もしくは第2の暗号化メディア鍵データを読み込む必要がないため、装置内に設けるメモリ容量を小さくでき、処理時間も短くできる。また、第1の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムを第2の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムと異なるものとすることができるため、第1のカテゴリの再生装置の無効化システムが暴露されるような事態に陥った場合にも、第1のカテゴリの再生装置に付与するデバイス鍵の鍵長や第1の暗号化メディア鍵データの生成アルゴリズムを変更することで、第2のカテゴリの再生装置に影響を与えることなく、無効化システムを変更することが可能になる。これは、本実施の形態のように第1のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される再生装置とし、第2のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される再生装置とした場合に、特に有効である。

【0069】

なお、本実施の形態では図1において、メディア鍵及びコンテンツ鍵が記録装置100の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、記録装置100がメディア鍵及びコンテンツ鍵を格納する格納部を有する構成であってもよい。また、記録装置100がメディア鍵及びコンテンツ鍵をその都度生成する生成部を有する構成であってもよい。

【0070】

また、本実施の形態では図1において、コンテンツをコンテンツ鍵で暗号化し、コンテンツ鍵をメディア鍵で暗号化する2階層の構成としたが、本発明はそれに限定されるものではない。例えば、メディア鍵で直接コンテンツを暗号化する1階層の構成であってもよい。また、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

【0071】

また、本実施の形態では記録装置として図1に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、コンテンツ鍵暗号化部、コンテンツ暗号化部及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではなく、記録装置が分離して構成されるものであっても良い。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、及びコンテンツ鍵暗号化部(図1中の破線で囲んだ部分)は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置される装置に内蔵され、コンテンツ暗号化部や記録媒体への各データの記録はコンテンツ製造機関や記録媒体製造機関に設置される装置で実行される形態であっても良い。

【0072】

また、本実施の形態ではシステム更新において第1の暗号化メディア鍵データを生成する際に、図5のEa(DKA' 2, 0)や図6のEa'(DKA' 2, 0)のようにシステム更新の時点で無効化されている再生装置にもデータを割り当てる構成としているが、無効化されている再生装置にはデータを割り当てない構成とすることも可能である。その場合、無効化されていない再生装置の使うべき暗号化メディア鍵の位置も更新し、新たな

デバイス鍵を付与する際に新たな位置情報も付与することで、システム更新の前後において暗号化メディア鍵の位置が変わったとしても無効化されていない再生装置は適切なデータを用いることができ、正しいメディア鍵を得ることができる。こうした場合、システム更新後の第1の暗号化メディア鍵データ記録領域に格納すべきデータの容量を削減することができる。あるいは容量の最大値が限定されている場合は新たに第1のカテゴリに属する再生装置の台数を増やすことが可能となる。

【0073】

また、本実施の形態では、図4に示すような暗号化メディア鍵データを用いて再生装置の無効化を行う方法としたが、無効化の方法は他の方法を利用してもよく、例えば特許文献1として開示されている木構造を利用した無効化方法を用いても良い。

【0074】

また、本実施の形態では、暗号アルゴリズムとして鍵長56bitのDES、あるいはシステム更新後の暗号アルゴリズムとして鍵長112bitの2キートリプルDESを用いたが、本発明はこれに限定されるものではなく、他の暗号アルゴリズム、例えば次世代の標準暗号とされる鍵長128bitのAES等を用いても良い。

【0075】

(実施の形態2)

本発明の実施の形態2は、書き換え型もしくは追記型の記録媒体に記録装置でコンテンツを記録し、再生装置でコンテンツを再生するシステムに本発明を適用したものである。

【0076】

以下、本発明の実施の形態2について、図面を参照しながら説明する。図7は、鍵情報を生成して記録する鍵生成装置700及び記録媒体720を示しており、図8は、記録媒体720にコンテンツを暗号化して記録する第1のカテゴリの記録装置800を示しており、図9は、記録媒体720にコンテンツを暗号化して記録する第2のカテゴリの記録装置900を示しており、図10は記録媒体720から暗号化コンテンツを読み出して復号する第1のカテゴリの再生装置1000を示しており、図11は記録媒体720から暗号化コンテンツを読み出して復号する第2のカテゴリの再生装置1100を示している。また、図12は、記録媒体720に記録される各種データの具体例を示している。

【0077】

鍵生成装置700は、第1のデバイス鍵格納部701に第1のカテゴリの各装置が秘密に保有するデバイス鍵を、第2のデバイス鍵格納部702に第2のカテゴリの各装置が秘密に保有するデバイス鍵を、それぞれ格納する。メディア鍵及びコンテンツ鍵の暗号化については、前記した実施の形態1における記録装置と同様であるので、その説明は省略する。

【0078】

記録媒体720は、第1の暗号化メディア鍵データ記録領域721と、第2の暗号化メディア鍵データ記録領域722と、暗号化コンテンツ鍵記録領域723と、暗号化コンテンツ記録領域724とを備える。ここで、破線で囲んだ、第1の暗号化メディア鍵データ記録領域721、第2の暗号化メディア鍵データ記録領域722、及び、暗号化コンテンツ鍵記録領域723は、第1のカテゴリの記録装置800及び第2のカテゴリの記録装置900では記録不可能な領域である。一方、暗号化コンテンツ記録領域は、第1のカテゴリの記録装置800及び第2のカテゴリの記録装置900で記録可能な領域である。

【0079】

第1のカテゴリの記録装置800は、デバイス鍵を秘密に保有するデバイス鍵格納部801と、デバイス鍵を用いて記録媒体720から読み出した第1の暗号化メディア鍵データを復号してメディア鍵を取得するメディア鍵復号部802と、取得したメディア鍵を用いて記録媒体から読み出した暗号化コンテンツ鍵を復号してコンテンツ鍵を取得するコンテンツ鍵復号部803と、取得したコンテンツ鍵を用いて外部から入力されたコンテンツを暗号化するコンテンツ暗号化部804とを備える。本実施の形態では、パソコン上のアプリケーションプログラムのようにソフトウェアで実装される記録装置を第1のカテゴリ

に属する記録装置とした。

【0080】

第2のカテゴリの記録装置900は、デバイス鍵を秘密に保有するデバイス鍵格納部901と、デバイス鍵を用いて記録媒体720から読み出した第2の暗号化メディア鍵データを復号してメディア鍵を取得するメディア鍵復号部902と、取得したメディア鍵を用いて記録媒体から読み出した暗号化コンテンツ鍵を復号してコンテンツ鍵を取得するコンテンツ鍵復号部903と、取得したコンテンツ鍵を用いて外部から入力されたコンテンツを暗号化するコンテンツ暗号化部904とを備える。本実施の形態では、一般的な民生レコーダのようにハードウェアで実装される記録装置を第2のカテゴリに属する記録装置とした。

【0081】

第1のカテゴリの再生装置1000及び第2のカテゴリの再生装置1100は、それぞれ前記した本発明の実施の形態1における第1のカテゴリの再生装置200及び第2のカテゴリの再生装置300と同じ構成であり、同一の構成要素には同一の符号を付し、その説明を省略する。

【0082】

図12は、m台の第1のカテゴリの装置、及びn台の第2のカテゴリの装置がそれぞれ固有のデバイス鍵を1個だけ保有しており、第1のカテゴリの装置2と第2のカテゴリの装置3が無効化されているとした場合の、記録媒体720に記録される各種データの具体例を示している。図12中で、第1のカテゴリの装置i ($i=1\sim m$) が保有するデバイス鍵をDKA_i、第2のカテゴリの装置j ($j=1\sim n$) が保有するデバイス鍵をDKB_jとしている。なお、第1の暗号化メディア鍵データ記録領域721、第2の暗号化メディア鍵データ記録領域722、暗号化コンテンツ鍵データ記録領域723、及び暗号化コンテンツ記録領域724に記録されるデータは、それぞれ前記した本発明の実施の形態1における第1の暗号化メディア鍵データ記録領域121、第2の暗号化メディア鍵データ記録領域122、暗号化コンテンツ鍵データ記録領域123、及び暗号化コンテンツ記録領域124に記録されるデータと同じであるので、その説明を省略する。

【0083】

本実施の形態によれば、上記した構成により、第1のカテゴリの装置2及び第2のカテゴリの装置3を除く装置が正しいメディア鍵(MK)を復号することができるとともに、第1のカテゴリの装置2及び第2のカテゴリの装置3をシステムから排除することができる。

【0084】

また、本実施の形態において、第1のカテゴリの装置の無効化が機能しなくなったと判断された場合には、第1のカテゴリの装置の無効化システムを更新することになる。更新の方法については、前記した本発明の実施の形態1の場合と同様の方法がとれるので、その説明を省略する。

【0085】

なお、システムの更新に際して、第2の暗号化メディア鍵の生成に用いるデバイス鍵(DKB₁~DKB_n)は変更されていないので、第2のカテゴリに属する記録装置及び再生装置には何らの変更を加える必要がない。

【0086】

以上のように構成された本発明の実施の形態2によれば、第1のカテゴリの装置(記録装置800及び再生装置1000)及び第2のカテゴリの装置(記録装置900及び再生装置1100)は、それぞれ異なるカテゴリの装置を無効化するための第1もしくは第2の暗号化メディア鍵データを読み込む必要がないため、装置内に設けるメモリ容量を小さくでき、処理時間も短くできる。また、第1の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムを第2の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムと異なるものとすることができるため、第1のカテゴリの装置の無効化システムが暴露されるような事態に陥った場合にも、第1のカテゴリの装置に付与するデバイス鍵の鍵長や第

1の暗号化メディア鍵データの生成アルゴリズムを変更することで、第2のカテゴリの装置に影響を与えることなく、無効化システムを変更することが可能になる。これは、本実施の形態のように第1のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される装置とし、第2のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される装置とした場合に、特に有効である。

【0087】

なお、本実施の形態では、各カテゴリの記録装置と再生装置が別々の装置である形態としたが、本発明はそれに限定されるものではない。例えば、記録装置と再生装置が同一の装置である形態であっても良い。

【0088】

また、本実施の形態では図7において、メディア鍵及びコンテンツ鍵が鍵生成装置700の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、鍵生成装置700がメディア鍵及びコンテンツ鍵を格納する格納部を有する構成であってもよい。また、鍵生成装置700がメディア鍵及びコンテンツ鍵をその都度生成する生成部を有する構成であってもよい。

【0089】

また、本実施の形態では図8及び図9において、メディア鍵で暗号化コンテンツ鍵を復号してコンテンツ鍵を取得し、取得したコンテンツ鍵でコンテンツを暗号化する2階層の構成としたが、本発明はそれに限定されるものではない。例えば、メディア鍵で直接コンテンツを暗号化する1階層の構成であってもよい。また、記録装置内部で生成したコンテンツ鍵を用いてコンテンツを暗号化し、コンテンツ鍵をメディア鍵で暗号化し、暗号化コンテンツと暗号化コンテンツ鍵を記録媒体に記録する構成であってもよい。また、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

【0090】

また、本実施の形態では鍵生成装置として図7に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、コンテンツ鍵暗号化部、及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではない。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、及びコンテンツ鍵暗号化部は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置される装置に内蔵され、記録媒体への各データの記録は記録媒体製造機関に設置される装置で実行される形態であっても良い。一般的に書き換え型もしくは追記型の光ディスクでは、一般ユーザの保有する記録装置で記録可能な領域と、一般ユーザの保有する記録装置では記録不可能な再生専用領域を備えており、この再生専用領域にはディスク製造業者が出荷前にデータを記録する。この場合、ディスク製造業者による再生専用領域へのデータ記録は、スタンパと呼ばれる原盤にデータを記録し、このスタンパを用いたプレス工程で行われるのが一般的である。このようなディスク製造業者による再生専用領域へのデータ記録工程において、暗号化メディア鍵データが記録媒体に記録される場合であっても本発明は適用可能である。

【0091】

(実施の形態3)

本発明の実施の形態3は、実施の形態1と同様、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものである。

【0092】

以下、本発明の実施の形態3について、図面を参照にしながら説明する。図13は、コンテンツを暗号化して記録する記録装置1300及び記録媒体1320を示しており、図14は、記録媒体1320から暗号化コンテンツを読み出して復号する第1のカテゴリの再生装置1400を示しており、図15は、記録媒体1320から暗号化コンテンツを読み出して復号する第2のカテゴリの再生装置1500を示している。また、図16は記録媒体1320に記録される各種データの具体例を示している。

【0093】

図13の記録装置1300が図1の記録装置100と異なる点は、第1のカテゴリに対しては第1のメディア鍵を、第2のカテゴリに対しては第2のメディア鍵を、個別に設け、第1及び第2のメディア鍵をそれぞれ第1のメディア鍵暗号化部1305及び第2のメディア鍵暗号化部1306で暗号化し、コンテンツ鍵を第1及び第2のメディア鍵を用いてそれぞれ第1のコンテンツ鍵暗号化部1307及び第2のコンテンツ鍵暗号化部1308で暗号化し、記録媒体1320に記録するようにしたことである。その他の点は図1の記録装置100と同じであるので、その説明は省略する。

【0094】

記録媒体1320は、第1のメディア鍵暗号化部1305が生成した第1の暗号化メディア鍵データを記録する第1の暗号化メディア鍵データ記録領域1321と、第2のメディア鍵暗号化部1306が生成した第2の暗号化メディア鍵データを記録する第2の暗号化メディア鍵データ記録領域1322と、第1のコンテンツ鍵暗号化部1307が生成した第1の暗号化コンテンツ鍵を記録する第1の暗号化コンテンツ鍵記録領域1323と、第2のコンテンツ鍵暗号化部1308が生成した第2の暗号化コンテンツ鍵を記録する第2の暗号化コンテンツ鍵記録領域1324と、コンテンツ暗号化部1309が生成した暗号化コンテンツを記録する暗号化コンテンツ記録領域1325とを備える。

【0095】

第1カテゴリの再生装置1400及び第2のカテゴリの再生装置1500は、それぞれ記録媒体1320から読み出した第1および第2の暗号化コンテンツ鍵を復号してコンテンツ鍵を取得する。その他の点については、実施の形態1における第1のカテゴリの再生装置200及び第2のカテゴリの再生装置300と同様であるので、その説明は省略する。

【0096】

図16は、m台の第1のカテゴリの再生装置及びn台の第2のカテゴリの再生装置がそれぞれ固有のデバイス鍵を1個だけ保有しており、第1のカテゴリの再生装置2と第2のカテゴリの再生装置3が無効化されているとした場合の、記録媒体1320に記録される各種データの具体例を示している。図16中で、第1のカテゴリの再生装置i (i=1~m) が保有するデバイス鍵をDKAi、第2のカテゴリの再生装置j (j=1~n) が保有するデバイス鍵をDKBjとしている。また、Ea(X, Y)、Eb(X, Y)、Ec(X, Y)、Ed(X, Y)及びEe(X, Y)はデータYを鍵データXを用いて暗号化する関数を意味する。なお、使用される暗号アルゴリズムは、公知の技術で実現可能であり、本実施の形態では鍵長56bitのDES暗号を使用した。

【0097】

(第1の暗号化メディア鍵データ記録領域1321)

第1の暗号化メディア鍵データ記録領域1321には、第1のカテゴリの再生装置が保有するデバイス鍵(DKA1~DKAm)で暗号化された第1のメディア鍵(MK1)が記録されている。ここで、第1のカテゴリの再生装置2は無効化されており、DKA2では第1のメディア鍵(MK1)とはまったく無関係のデータ「0」が暗号化されて記録されている。これは第1の暗号化メディア鍵データを生成する際に、第1のメディア鍵暗号化部1305において、第1のカテゴリのうち無効化すべき再生装置の情報として再生装置2が入力され、再生装置2では正しいメディア鍵が得られないように処理された結果である。第1の暗号化メディア鍵データをこのように生成することにより、再生装置2を除く第1のカテゴリの再生装置が正しい第1のメディア鍵(MK1)を復号することができ、再生装置2をシステムから排除することができる。

【0098】

(第2の暗号化メディア鍵データ記録領域1322)

第2の暗号化メディア鍵データ記録領域1322には、第2のカテゴリの再生装置が保有するデバイス鍵(DKB1~DKBn)で暗号化された第2のメディア鍵(MK2)が記録されている。ここで、第2のカテゴリの再生装置3は無効化されており、DKB3で

は第2のメディア鍵(MK2)とはまったく無関係のデータ「0」が暗号化されて記録されている。これは第2の暗号化メディア鍵データを生成する際に、第2のメディア鍵暗号化部1306において、第2のカテゴリのうち無効化すべき再生装置の情報として再生装置3が入力され、再生装置3では正しいメディア鍵が得られないように処理された結果である。第2の暗号化メディア鍵データをこのように生成することにより、再生装置3を除く第2のカテゴリの再生装置が正しい第2のメディア鍵(MK2)を復号することができ、再生装置3をシステムから排除することができる。

【0099】

(第1の暗号化コンテンツ鍵記録領域1323)

第1の暗号化コンテンツ鍵記録領域1323には第1のメディア鍵(MK1)で暗号化されたコンテンツ鍵(CK)が記録されている。

【0100】

(第2の暗号化コンテンツ鍵記録領域1324)

第2の暗号化コンテンツ鍵データ記録領域1324には第2のメディア鍵(MK2)で暗号化されたコンテンツ鍵(CK)が記録されている。

【0101】

(暗号化コンテンツ記録領域1325)

暗号化コンテンツ記録領域1325には、コンテンツ鍵(CK)で暗号化されたコンテンツが記録されている。

【0102】

以上のように構成された本発明の実施の形態1において、例えば第1のカテゴリの再生装置に付与したデバイス鍵の多数や、第1の暗号化メディア鍵及び第1の暗号化コンテンツ鍵を復号するアルゴリズムがインターネット上で不正に公開され、第1のカテゴリの再生装置の無効化が機能しなくなったと判断された場合には、第1のカテゴリの再生装置の無効化システムを更新することになる。以下、その具体例を説明する。

【0103】

(システム更新の具体例1)

第1のカテゴリの再生装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体1320に記録する各種データの具体例1を図17に示す。図16との違いは、第1の暗号化メディア鍵データの生成に用いるデバイス鍵をDKA1~DKAmからDKA'1~DKA'mに変更したことである。これは、前記した実施の形態1で述べたシステム更新の具体例1と同様であるので、詳細についての説明は省略する。

【0104】

ここで、新たなデバイス鍵(DKA'1~DKA'm)のうちの各デバイス鍵は、システム更新前のデバイス鍵(DKA1~DKAm)のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵がDKA2以外に存在したとしても、そのデバイス鍵を使って図17の記録媒体から読み出した第1の暗号化メディア鍵データを復号してメディア鍵(MK1)を取得することはできず、コンテンツを再生することはできない。

【0105】

なお、上記したシステム更新に際して、第2の暗号化メディア鍵データの生成に用いるデバイス鍵(DKB1~DKBn)は変更されていないので、第2のカテゴリに属する再生装置には何らの変更を加える必要がない。

【0106】

(システム更新の具体例2)

第1のカテゴリの再生装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体1320に記録する各種データの具体例2を図18に示す。図16との違いは、第1の暗号化メディア鍵データの生成に用いるデバイス鍵をDKA1~DKAmからDKA'1~DKA'mに変更したこと、第1の暗号化メディア鍵データの暗号化アルゴリズムをEa(X,Y)からEa'(X,Y)に変更したこと、第1の暗号化コンテンツ

鍵の暗号化アルゴリズムを $E_c(X, Y)$ から $E_{c'}(X, Y)$ に変更したことである。ここで、新たなデバイス鍵($DKA'_1 \sim DKA'_m$)のうちの各デバイス鍵は、システム更新前のデバイス鍵($DKA_1 \sim DKA_m$)のどれとも一致しないようになっている。

【0107】

一方、無効化されていない第1のカテゴリの各再生装置1400には、新たなデバイス鍵を付与されデバイス鍵格納部1401に格納される。メディア鍵復号部1402には、以前から組み込まれている図16の第1の暗号化メディア鍵を復号するための復号アルゴリズム $Da(X, Y)$ に加えて、図18の第1の暗号化メディア鍵を復号するための復号アルゴリズム $Da'(X, Y)$ が組み込まれる。また、コンテンツ鍵復号部1403には、以前から組み込まれている図16の第1の暗号化コンテンツ鍵を復号するための復号アルゴリズム $Dc(X, Y)$ に加えて、図18の第1の暗号化コンテンツ鍵を復号するための復号アルゴリズム $Dc'(X, Y)$ が組み込まれる。例えば、第1のカテゴリの再生装置 m は、以前から保有していたデバイス鍵(DKA_m)に加え、新たに付与されたデバイス鍵(DKA'_m)を保有する。再生装置 m は、図16の記録媒体を再生する際には、デバイス鍵 DKA_m と暗号化アルゴリズム $Da(X, Y)$ を用いて、第1の暗号化メディア鍵データを復号して第1のメディア鍵(MK_1)を取得し、取得した第1のメディア鍵(MK_1)と暗号化アルゴリズム $Dc(X, Y)$ を用いて第1の暗号化コンテンツ鍵を復号してコンテンツ鍵(CK)を取得し、取得したコンテンツ鍵(CK)を用いて暗号化コンテンツを復号する。一方、図18の記録媒体を再生する際には、デバイス鍵 DKA'_m と暗号アルゴリズム $Da'(X, Y)$ を用いて、第1の暗号化メディア鍵データを復号してメディア鍵(MK_1)を取得し、取得したメディア鍵(MK_1)と暗号化アルゴリズム $Dc'(X, Y)$ を用いて第1の暗号化コンテンツ鍵を復号してコンテンツ鍵(CK)を取得し、取得したコンテンツ鍵(CK)を用いて暗号化コンテンツを復号する。本実施の形態では $E_a(X, Y)$ 、 $Da(X, Y)$ 、 $E_c(X, Y)$ 及び $Dc(X, Y)$ は鍵長56bitのDES暗号を用いたのに対して、 $E_{a'}(X, Y)$ 、 $Da'(X, Y)$ 、 $E_{c'}(X, Y)$ 及び $Dc'(X, Y)$ 、では2キートリプルDESと呼ばれる鍵長112bitの暗号を用いた。

【0108】

ここで、新たなデバイス鍵($DKA'_1 \sim DKA'_m$)のうちの各デバイス鍵は、システム更新前のデバイス鍵($DKA_1 \sim DKA_m$)のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵が DKA_2 以外に存在したとしても、そのデバイス鍵を使って図18の記録媒体から読み出した第1の暗号化メディア鍵データを復号してメディア鍵(MK_1)を取得することはできず、コンテンツを再生することはできない。

【0109】

また、デバイス鍵の鍵長や暗号アルゴリズムを変更して暗号強度の高いものにすることができるので、システムを解析してデバイス鍵を不正取得するといった行為を困難にすることができる。

【0110】

なお、上記したシステム更新に際して、第2の暗号化メディア鍵データの生成に用いるデバイス鍵($DKB_1 \sim DKB_n$)、第2の暗号化メディア鍵データの暗号化アルゴリズム、及び第2の暗号化コンテンツ鍵データの暗号化アルゴリズムは変更されていないので、第2のカテゴリに属する再生装置には何らの変更を加える必要がない。

【0111】

以上のように構成された本発明の実施の形態3によれば、第1のカテゴリの再生装置1400及び第2のカテゴリの再生装置1500は、それぞれ異なるカテゴリの再生装置を無効化するための第1もしくは第2の暗号化メディア鍵データを読み込む必要がないため、装置内に設けるメモリ容量を小さくでき、処理時間も短くできる。また、第1の暗号化メディア鍵データ及び第1の暗号化コンテンツ鍵の生成に用いる暗号化アルゴリズムを、それぞれ第2の暗号化メディア鍵データ及び第2の暗号化コンテンツ鍵の生成に用いる暗

号化アルゴリズムと異なるものとするができるため、第1のカテゴリの再生装置の無効化システムが暴露されるような事態に陥った場合にも、第1のカテゴリの再生装置に付与するデバイス鍵の鍵長や第1の暗号化メディア鍵データの生成アルゴリズムを変更することで、第2のカテゴリの再生装置に影響を与えることなく、無効化システムを変更することが可能になる。

【0112】

また、本実施の形態では第1のカテゴリと第2のカテゴリに対して個別にメディア鍵を設け、それぞれを用いた暗号化コンテンツ鍵の階層を設けることにより、カテゴリ間の独立性を高めることが可能となる。すなわち第1のカテゴリに属する再生装置からデバイス鍵が暴露された場合であっても、それを用いて得られるメディア鍵は第1のメディア鍵のみであり、第2のメディア鍵が暴露されることを防ぐことが可能となる。これは、本実施の形態のように第1のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される再生装置とし、第2のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される再生装置とした場合に、特に有効である。

【0113】

なお、図13では、第1のメディア鍵、第2のメディア鍵及びコンテンツ鍵が記録装置1300の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、記録装置1300が第1のメディア鍵、第2のメディア鍵及びコンテンツ鍵を格納する格納部を有する構成であってもよい。また、記録装置1300が第1のメディア鍵、第2のメディア鍵及びコンテンツ鍵をその都度生成する生成部を有する構成であってもよい。

【0114】

また、図13では、コンテンツをコンテンツ鍵で暗号化し、コンテンツ鍵を第1及び第2のメディア鍵で暗号化する2階層の構成としたが、本発明はそれに限定されるものではない。例えば、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

【0115】

また、本実施の形態では記録装置として図13に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、コンテンツ鍵暗号化部、コンテンツ暗号化部及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではない。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、コンテンツ鍵暗号化部（図13中の破線で囲んだ部分）は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置される装置に内蔵され、コンテンツ暗号部や記録媒体への各データの記録はコンテンツ製造機関や記録媒体製造機関に設置される装置で実行される形態であっても良い。

【0116】

また、本実施の形態ではシステム更新において第1の暗号化メディア鍵データを生成する際に、図17のEa(DKA' 2, 0)や図18のEa'(DKA' 2, 0)のようにシステム更新の時点で無効化されている再生装置にもデータを割り当てる構成としているが、無効化されている再生装置にはデータを割り当てない構成とすることも可能である。その場合、無効化されていない再生装置の使うべき暗号化メディア鍵の位置も更新し、新たなデバイス鍵を付与する際に新たな位置情報も付与することで、システム更新の前後において暗号化メディア鍵の位置が変わったとしても無効化されていない再生装置は適切なデータを用いることができ、正しいメディア鍵を得ることができる。こうした場合、システム更新後の第1の暗号化メディア鍵データ記録領域に格納すべきデータの容量を削減することができる。あるいは容量の最大値が限定されている場合は新たに第1のカテゴリに属する再生装置の台数を増やすことが可能となる。

【0117】

また、本実施の形態では、図16に示すような暗号化メディア鍵データを用いて再生装置の無効化を行う方法としたが、無効化の方法は他の方法を利用してもよく、例えば特許

文献1として開示されている木構造を利用した無効化方法を用いても良い。

【0118】

また、本実施の形態では、暗号アルゴリズムとして鍵長56bitのDES、あるいはシステム更新後の暗号アルゴリズムとして鍵長112bitの2キートリプルDESを用いたが、本発明はこれに限定されるものではなく、他の暗号アルゴリズム、例えば次世代の標準暗号とされる鍵長128bitのAES等を用いても良い。

【0119】

なお、本実施の形態は、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものであるが、本発明はこれに限定されるものではない。前記した実施の形態2のように、鍵生成装置で各カテゴリ用の暗号化メディア鍵データ及び暗号化コンテンツ鍵を生成して記録媒体に記録し、記録装置で暗号化メディア鍵データ及び暗号化コンテンツ鍵を復号してコンテンツを暗号化する構成とすることにより、書き換え型もしくは追記型の記録媒体を用いるシステムにも適用することができる。

【0120】

(実施の形態4)

本発明の実施の形態4は、実施の形態1と同様、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものである。

【0121】

以下、本発明の実施の形態4について、図面を参照にしながら説明する。図19は、コンテンツを暗号化して記録する記録装置1900及び記録媒体1920を示しており、図20は、記録媒体1920から暗号化コンテンツを読み出して復号する第1の再生装置2000を示しており、図21は、記録媒体1920から暗号化コンテンツを読み出して復号する第2の再生装置2100を示している。また、図22は記録媒体1920に記録される各種データの具体例を示している。

【0122】

図19の記録装置1900が図1の記録装置100と異なる点は、コンテンツに対して第1のコンテンツ鍵を用いて第1のコンテンツ暗号化部1909で第1のコンテンツ暗号化を施し、その出力に対して第2のコンテンツ鍵を用いて第2のコンテンツ暗号化部1910で第2のコンテンツ暗号化を施し、メディア鍵を用いて第1及び第2のコンテンツ鍵をそれぞれ第1のコンテンツ鍵暗号化部1907及び第2のコンテンツ鍵暗号化部1908で暗号化し、記録媒体1920に記録するようにしたことである。その他の点は図1の記録装置100と同じであるので、その説明は省略する。

【0123】

記録媒体1920は、第1の暗号化メディア鍵データを記録する第1の暗号化メディア鍵データ記録領域1921と、第2の暗号化メディア鍵データを記録する第2の暗号化メディア鍵データ記録領域1922と、第1のコンテンツ鍵暗号化部1907が生成した第1の暗号化コンテンツ鍵を記録する第1の暗号化コンテンツ鍵記録領域1923と、第2のコンテンツ鍵暗号化部1908が生成した第2の暗号化コンテンツ鍵を記録する第2の暗号化コンテンツ鍵記録領域1924と、第2のコンテンツ暗号化部1910が生成した暗号化コンテンツを記録する暗号化コンテンツ記録領域1925とを備える。

【0124】

第1の再生装置2000は、読み出し装置2010及び復号装置2020とから構成される。

【0125】

読み出し装置2010は、デバイス鍵を秘密に保有するデバイス鍵格納部2011と、デバイス鍵を用いて記録媒体1920から読み出した第2の暗号化メディア鍵データを復号してメディア鍵を取得する第2のメディア鍵復号部2012と、取得したメディア鍵を用いて記録媒体から読み出した第2の暗号化コンテンツ鍵を復号してコンテンツ鍵を取得する第2のコンテンツ鍵復号部2013と、取得したコンテンツ鍵を用いて記録媒体19

20から読み出した暗号化コンテンツに第2のコンテンツ復号処理を施す第2のコンテンツ復号部2014とを備え、第2のコンテンツ復号部2014で暗号化コンテンツに第2の復号処理を施した結果の中間データを記録媒体1920から読み出した第1の暗号化メディア鍵データ及び第1の暗号化コンテンツ鍵とともに復号装置2020に供給する。本実施の形態において、読み出し装置2010は上記した構成要素がハードウェアで実装されており、第2のカテゴリに属するものとした。

【0126】

復号装置2020は、デバイス鍵を秘密に保有するデバイス鍵格納部2021と、デバイス鍵を用いて読み出し装置2010から供給される第1の暗号化メディア鍵データを復号してメディア鍵を取得する第1のメディア鍵復号部2022と、取得したメディア鍵を用いて読み出し装置2010から供給される第1の暗号化コンテンツ鍵を復号して第1のコンテンツ鍵を取得する第1のコンテンツ鍵復号部2023と、取得した第1のコンテンツ鍵を用いて読み取り装置2010から供給される中間データに第1のコンテンツ復号処理を施してコンテンツを取得する第1のコンテンツ復号部2024とを備える。本実施の形態において、復号装置2020は上記した構成要素がソフトウェアで実装されており、第1のカテゴリに属するものとした。

【0127】

第2の再生装置2100は、第2のカテゴリの再生装置であり、デバイス鍵を秘密に保有するデバイス鍵格納部2101と、デバイス鍵を用いて記録媒体1920から読み出した第2の暗号化メディア鍵データを復号してメディア鍵を取得するメディア鍵復号部2102と、取得したメディア鍵を用いて記録媒体から読み出した第2の暗号化コンテンツ鍵を復号して第2のコンテンツ鍵を取得する第2のコンテンツ鍵復号部2103と、取得した第2のコンテンツ鍵を用いて記録媒体1920から読み出した暗号化コンテンツに第2のコンテンツ復号処理を施す第2のコンテンツ復号部2104と、取得したメディア鍵を用いて記録媒体から読み出した第1の暗号化コンテンツ鍵データを復号して第1のコンテンツ鍵を取得する第1のコンテンツ鍵復号部2105と、第2のコンテンツ復号部2104の出力に第1のコンテンツ鍵を用いて第1のコンテンツ復号処理を施してコンテンツを取得する第1のコンテンツ復号部2106とを備える。本実施の形態において、第2の再生装置2100は、上記した構成要素がハードウェアで実装されており、第2のカテゴリに属するものとした。

【0128】

本実施の形態ではパソコン上のアプリケーションプログラムのようにソフトウェアで実装される復号装置を第1のカテゴリに属する復号装置とし、一般的な民生プレーヤ及びパソコンに接続もしくは内蔵される光ディスクドライブのようにハードウェアで実装される装置を第2のカテゴリに属する装置とした。

【0129】

図22は、m台の第1のカテゴリの復号装置及びn台の第2のカテゴリの装置がそれぞれ固有のデバイス鍵を1個だけ保有しており、第1のカテゴリの復号装置2と第2のカテゴリの装置3が無効化されているとした場合の、記録媒体1920に記録される各種データの具体例を示している。図22中で、第1のカテゴリの復号装置 i ($i=1\sim m$) が保有するデバイス鍵を DKA_i 、第2のカテゴリの装置 j ($j=1\sim n$) が保有するデバイス鍵を DKA_j としている。また、 $E_a(X, Y)$ 、 $E_b(X, Y)$ 、 $E_c(X, Y)$ 、 $E_d(X, Y)$ 、 $E_e(X, Y)$ 及び $E_f(X, Y)$ はデータYを鍵データXを用いて暗号化する関数を意味する。なお、使用される暗号アルゴリズムは公知の技術で実現可能であり、本実施の形態では鍵長56ビットのDES暗号を使用した。

【0130】

第1の暗号化メディア鍵データ記録領域1921及び第2の暗号化メディア鍵データ記録領域1922に記録されるデータは、それぞれ、前記した実施の形態1における第1の暗号化メディア鍵データ記録領域121及び第2の暗号化メディア鍵データ記録領域122に記録されるデータと同じであるので、その説明は省略する。

【0131】

(第1の暗号化コンテンツ鍵記録領域1923)

第1の暗号化コンテンツ鍵記録領域1923にはメディア鍵(MK)で暗号化された第1のコンテンツ鍵(CK1)が記録されている。

【0132】

(第2の暗号化コンテンツ鍵記録領域1924)

第2の暗号化コンテンツ鍵記録領域1924にはメディア鍵(MK)で暗号化された第2のコンテンツ鍵(CK2)が記録されている。

【0133】

(暗号化コンテンツ記録領域1925)

暗号化コンテンツ記録領域1925には、第1のコンテンツ鍵(CK1)及び第2のコンテンツ鍵(CK2)で暗号化されたコンテンツが記録されている。

【0134】

以上のように構成された本発明の実施の形態4において、例えば第1のカテゴリの復号装置に付与したデバイス鍵の多数や、第1の暗号化メディア鍵データを復号するアルゴリズムがインターネット上で不正に公開され、第1のカテゴリの復号装置の無効化が機能しなくなったと判断された場合には、第1のカテゴリの復号装置の無効化システムを更新することになる。以下、その具体例を説明する。

【0135】

(システム更新の具体例1)

第1のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体1920に記録する各種データの具体例1を図23に示す。図22との違いは、第1の暗号化メディア鍵の生成に用いるデバイス鍵をDKA1~DKAmからDKA'1~DKA'mに変更したことである。これは、前記した実施の形態1で述べたシステム更新の具体例1と同様であるので、詳細についての説明は省略する。

【0136】

ここで、新たなデバイス鍵(DKA'1~DKA'm)のうちの各デバイス鍵は、システム更新前のデバイス鍵(DKA1~DKAm)のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵がDKA2以外に存在したとしても、そのデバイス鍵を使って図23の記録媒体から読み出した第1の暗号化メディア鍵データを復号してメディア鍵(MK)を取得することはできず、コンテンツを再生することはできない。

【0137】

なお、上記したシステム更新に際して、第2の暗号化メディア鍵データの生成に用いるデバイス鍵(DKB1~DKBn)は変更されていないので、第2のカテゴリに属する装置には何らの変更を加える必要がない。

【0138】

(システム更新の具体例2)

第1のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体1920に記録する各種データの具体例2を図24に示す。図22との違いは、第1の暗号化メディア鍵データの生成に用いるデバイス鍵をDKA1~DKAmからDKA'1~DKA'mに変更したことと、暗号化アルゴリズムをEa(X,Y)からEa'(X,Y)に変更したことである。これは、前記した実施の形態1で述べたシステム更新の具体例2と同様であるので、詳細についての説明は省略する。

【0139】

ここで、新たなデバイス鍵(DKA'1~DKA'm)のうちの各デバイス鍵は、システム更新前のデバイス鍵(DKA1~DKAm)のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵がDKA2以外に存在したとしても、そのデバイス鍵を使って図24の記録媒体から読み出した第1の暗号化メディア鍵データを復号してメディア鍵(MK)を取得することはできず、コンテンツを

再生することはできない。

【0140】

また、デバイス鍵の鍵長や暗号アルゴリズムを変更して暗号強度の高いものにすることができ、システムを解析してデバイス鍵を不正取得するといった行為を困難にすることができる。

【0141】

なお、上記したシステム更新に際して、第2の暗号化メディア鍵データの生成に用いるデバイス鍵（DKB1～DKBn）及び第2の暗号化メディア鍵データの暗号化アルゴリズムは変更されていないので、第2のカテゴリに属する装置には何らの変更を加える必要がない。

【0142】

以上のように構成された本発明の実施の形態4によれば、第1のカテゴリの装置（復号装置2020）及び第2のカテゴリの装置（読み出し装置2010及び第2の再生装置2100）は、それぞれ異なるカテゴリの装置を無効化するための第1もしくは第2の暗号化メディア鍵データを読み込む必要がないため、装置内に設けるメモリ容量を小さくでき、処理時間も短くできる。また、第1の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムを第2の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムと異なるものとすることができるため、第1のカテゴリの復号装置の無効化システムが暴露されるような事態に陥った場合にも、第1のカテゴリの復号装置に付与するデバイス鍵の鍵長や第1の暗号化メディア鍵データの生成アルゴリズムを変更することで、第2のカテゴリの装置に影響を与えることなく、無効化システムを変更することが可能になる。さらに、第1のカテゴリの復号装置2020には、第2の暗号化コンテンツ鍵を復号するためのアルゴリズムは実装されていないので、第1のカテゴリの復号装置の何れかを解析して保有するデバイス鍵や復号アルゴリズムを暴露したとしても、コンテンツの復号に必要な全ての情報を取得することはできず、より堅牢な著作権保護システムを構築できる。これは、本実施の形態のように第1のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される復号装置とし、第2のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される再生装置もしくは読み取り装置とした場合に、特に有効である。

【0143】

なお、図19で、メディア鍵、第1のコンテンツ鍵、及び第2のコンテンツ鍵が記録装置1900の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、記録装置1900がメディア鍵、第1のコンテンツ鍵、及び第2のコンテンツ鍵を格納する格納部を有する構成であってもよい。また、記録装置1900がメディア鍵、第1のコンテンツ鍵、及び第2のコンテンツ鍵をその都度生成する生成部を有する構成であってもよい。

【0144】

また、図19では、コンテンツを第1及び第2のコンテンツ鍵で暗号化し、第1及び第2のコンテンツ鍵をメディア鍵で暗号化する2階層の構成としたが、本発明はそれに限定されるものではない。例えば、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

【0145】

また、本実施の形態では記録装置として図19に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、コンテンツ鍵暗号化部、コンテンツ暗号化部及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではなく、記録装置が分離して構成されるものであっても良い。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、及びコンテンツ鍵暗号化部（図19中の破線で囲んだ部分）は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置される装置に内蔵され、コンテンツ暗号部や記録媒体に各データへの記録はコンテンツ製造機関や記録媒体製造機関に設置される装置で実

行される形態であっても良い。

【0146】

また、本実施の形態ではシステム更新において第1の暗号化メディア鍵データを生成する際に、図23のEa(DKA' 2, 0)や図24のEa'(DKA' 2, 0)のようにシステム更新の時点で無効化されている復号装置にもデータを割り当てる構成としているが、無効化されている復号装置にはデータを割り当てない構成とすることも可能である。その場合、無効化されていない復号装置の使うべき暗号化メディア鍵の位置も更新し、新たなデバイス鍵を付与する際に新たな位置情報も付与することで、システム更新の前後において暗号化メディア鍵の位置が変わったとしても無効化されていない復号装置は適切なデータを用いることができ、正しいメディア鍵を得ることができる。こうした場合、システム更新後の第1の暗号化メディア鍵データ記録領域に格納すべきデータの容量を削減することができる。あるいは容量の最大値が限定されている場合は新たに第1のカテゴリに属する復号装置の台数を増やすことが可能となる。

【0147】

また、本実施の形態では、図22に示すような暗号化メディア鍵データを用いて復号装置の無効化を行う方法としたが、無効化の方法は他の方法を利用してもよく、例えば特許文献1として開示されている木構造を利用した無効化方法を用いても良い。

【0148】

また、本実施の形態では、暗号アルゴリズムとして鍵長56bitのDES、あるいはシステム更新後の暗号アルゴリズムとして鍵長112bitの2キートリプルDESを用いたが、本発明はこれに限定されるものではなく、他の暗号アルゴリズム、例えば次世代の標準暗号とされる鍵長128bitのAES等を用いても良い。

【0149】

また、図22では、コンテンツ全体を第1のコンテンツ鍵(CK1)で暗号化した後、さらに第2のコンテンツ鍵(CK2)で暗号化するようにしたが、本発明はそれに限定されるものではない。例えば、コンテンツを複数のブロックに分割したうちのいくつかのブロックを第1のコンテンツ鍵(CK1)で暗号化し、他のブロックを第2のコンテンツ鍵(CK2)で暗号化するようにしてもよい。

【0150】

なお、本実施の形態は、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものであるが、本発明はそれに限定されるものではない。前記した実施の形態2のように、鍵生成装置で各カテゴリ用の暗号化メディア鍵データ及び暗号化コンテンツ鍵を生成して記録媒体に記録し、記録装置で暗号化メディア鍵データ及び暗号化コンテンツ鍵を復号してコンテンツを暗号化する構成とすることにより、書き換え型もしくは追記型の記録媒体を用いるシステムにも適用することができる。

【0151】

(実施の形態5)

本発明の実施の形態5は、実施の形態4のシステムにおいて、第1のカテゴリと第2のカテゴリに対して個別にメディア鍵を設け、それぞれを用いた第1の暗号化コンテンツ鍵の階層を設けるようにしたものである。

【0152】

以下、本発明の実施の形態5について、図面を参照しながら説明する。図25は、コンテンツを暗号化して記録する記録装置2500及び記録媒体2520を示しており、図26は、記録媒体2520から暗号化コンテンツを読み出して復号する第1の再生装置2600を示しており、図27は、記録媒体2520から暗号化コンテンツを読み出して復号する第2の再生装置2700を示している。また、図28は記録媒体2520に記録される各種データの具体例を示している。

【0153】

図25の記録装置2500が図19の記録装置1900と異なる点は、第1のカテゴリ

に対しては第1のメディア鍵を、第2のカテゴリに対しては第2のメディア鍵を、個別に設け、第1及び第2のメディア鍵をそれぞれ第1のメディア鍵暗号化部2505及び第2のメディア鍵暗号化部2506で暗号化し、第1のコンテンツ鍵を第1及び第2のメディア鍵を用いてそれぞれ第1コンテンツ鍵暗号化部(1)2507及び第1のコンテンツ鍵暗号化部(2)2511で暗号化し、記録媒体2520に記録するようにしたことである。その他の点については、前記した実施の形態4の記録装置1900と同じであるので、その説明は省略する。

【0154】

記録媒体2520は、第1の暗号化メディア鍵データを記録する第1の暗号化メディア鍵データ記録領域2521と、第2の暗号化メディア鍵データを記録する第2の暗号化メディア鍵データ記録領域2522と、第1のコンテンツ鍵暗号化部(1)2507が生成した第1の暗号化コンテンツ鍵(1)を記録する第1の暗号化コンテンツ鍵(1)記録領域2523と、第1のコンテンツ鍵暗号化部(2)2511が生成した第1の暗号化コンテンツ鍵(2)を記録する第1の暗号化コンテンツ鍵(2)記録領域2526と、第2の暗号化コンテンツ鍵を記録する第2の暗号化コンテンツ鍵記録領域2524と、暗号化コンテンツを記録する暗号化コンテンツ記録領域2525とを備える。

【0155】

第1の再生装置2600において復号装置2620は、読み出し装置2610が記録媒体2520から読み出した第1の暗号化コンテンツ鍵(1)を復号して第1のコンテンツ鍵を取得する。その他の点については、前記した実施の形態4における第1の再生装置2000と同様であるので、その説明は省略する。

【0156】

第2の再生装置2700は、記録媒体2520から読み出した第1の暗号化コンテンツ鍵(2)を復号して第1のコンテンツ鍵を取得する。その他の点については、前記した実施の形態4における第2の再生装置2100と同様であるので、その説明は省略する。

【0157】

図28は、記録媒体2520に記録される各種データ的具体例を示している。第1の暗号化メディア鍵データ記録領域2521には、第1のカテゴリの復号装置が保有するデバイス鍵(DKA1~DKAm)で暗号化された第1のメディア鍵(MK1)が記録されており、第2の暗号化メディア鍵データ記録領域2522には、第2のカテゴリの装置が保有するデバイス鍵(DKB1~DKBm)で暗号化された第2のメディア鍵(MK2)がきろくされている。また、第1の暗号化コンテンツ鍵(1)記録領域2523には、第1のメディア鍵(MK1)で暗号化された第1のコンテンツ鍵(CK1)が記録されており、第1の暗号化コンテンツ鍵(2)記録領域2526には、第2のメディア鍵(MK2)で暗号化された第1のコンテンツ鍵(CK1)が記録されている。その他の点については、前記した図22と同じであるので、説明を省略する。なお、図28中の、Eg(X,Y)はデータYを鍵データXを用いて暗号化する関数を意味し、本実施の形態では鍵長56ビットのDES暗号を使用した。

【0158】

以上のように構成された本発明の実施の形態5において、例えば第1のカテゴリの復号装置に付与したデバイス鍵の多数や、第1の暗号化メディア鍵を復号するアルゴリズムがインターネット上で不正に公開され、第1のカテゴリの復号装置の無効化が機能しなくなったと判断された場合には、第1のカテゴリの復号装置の無効化システムを更新することになる。以下、その具体例を説明する。

【0159】

(システム更新の具体例1)

第1のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体2520に記録する各種データ的具体例1を図29に示す。図28との違いは、第1の暗号化メディア鍵データの生成に用いるデバイス鍵をDKA1~DKAmからDKA'1~DKA'mに変更したことである。これは、前記した実施の形態1で述べ

たシステム更新の具体例1と同様であるので、詳細についての説明は省略する。

【0160】

(システム更新の具体例2)

第1のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体2520に記録する各種データの具体例2を図30に示す。図22との違いは、第1の暗号化メディア鍵データの生成に用いるデバイス鍵をDKA1~DKAmからDKA'1~DKA'mに変更したこと、暗号化アルゴリズムをEa(X, Y)からEa'(X, Y)に変更したこと、及び第1の暗号化コンテンツ鍵(1)の暗号化アルゴリズムをEc(X, Y)からEc'(X, Y)に変更したことである。これは、前記した実施の形態3で述べたシステム更新の具体例2と同様であるので、詳細についての説明は省略する。

【0161】

以上のように構成された本発明の実施の形態5によれば、前記した実施の形態4同様に、堅牢な著作権保護システムを構築できる。さらに、本実施の形態では第1のカテゴリと第2のカテゴリに対して個別にメディア鍵を設け、それぞれを用いた暗号化コンテンツ鍵の階層を設けることにより、カテゴリ間の独立性を高めることが可能となる。すなわち第1のカテゴリに属する装置からデバイス鍵が暴露された場合であっても、それを用いて得られるメディア鍵は第1のメディア鍵のみであり、第2のメディア鍵が暴露されることを防ぐことが可能となる。これは、本実施の形態のように第1のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される復号装置とし、第2のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される再生装置もしくは読み取り装置とした場合に、特に有効である。

【0162】

なお、図25で、第1のメディア鍵、第2のメディア鍵、第1のコンテンツ鍵、及び第2のコンテンツ鍵が記録装置2500の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、記録装置2500がこれらの鍵を格納する格納部を有する構成であってもよい。また、記録装置2500がこれらの鍵をその都度生成する生成部を有する構成であってもよい。

【0163】

また、図25では、コンテンツを第1及び第2のコンテンツ鍵で暗号化し、第1及び第2のコンテンツ鍵をメディア鍵で暗号化する構成としたが、本発明はそれに限定されるものではない。例えば、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

【0164】

また、本実施の形態では記録装置として図25に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、コンテンツ鍵暗号化部、コンテンツ暗号化部及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではなく、記録装置が分離して構成されるものであっても良い。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、及びコンテンツ鍵暗号化部(図25中の破線で囲んだ部分)は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置される装置に内蔵され、コンテンツ暗号部や記録媒体に各データへの記録はコンテンツ製造機関や記録媒体製造機関に設置される装置で実行される形態であっても良い。

【0165】

また、本実施の形態ではシステム更新において第1の暗号化メディア鍵データを生成する際に、図29のEa(DKA'2, 0)や図30のEa'(DKA'2, 0)のようにシステム更新の時点で無効化されている復号装置にもデータを割り当てる構成としているが、無効化されている復号装置にはデータを割り当てない構成とすることも可能である。その場合、無効化されていない復号装置の使うべき暗号化メディア鍵の位置も更新し、新たなデバイス鍵を付与する際に新たな位置情報も付与することで、システム更新の前後に

において暗号化メディア鍵の位置が変わったとしても無効化されていない復号装置は適切なデータを用いることができ、正しいメディア鍵を得ることができる。こうした場合、システム更新後の第1の暗号化メディア鍵データ記録領域に格納すべきデータの容量を削減することができる。あるいは容量の最大値が限定されている場合は新たに第1のカテゴリに属する復号装置の台数を増やすことが可能となる。

【0166】

また、本実施の形態では、図28に示すような暗号化メディア鍵データを用いて復号装置の無効化を行う方法としたが、無効化の方法は他の方法を利用してもよく、例えば特許文献1として開示されている木構造を利用した無効化方法を用いても良い。

【0167】

また、本実施の形態では、暗号アルゴリズムとして鍵長56bitのDES、あるいはシステム更新後の暗号アルゴリズムとして鍵長112bitの2キートリプルDESを用いたが、本発明はこれに限定されるものではなく、他の暗号アルゴリズム、例えば次世代の標準暗号とされる鍵長128bitのAES等を用いても良い。

【0168】

また、図28では、コンテンツ全体を第1のコンテンツ鍵（CK1）で暗号化した後、さらに第2のコンテンツ鍵（CK2）で暗号化するようにしたが、本発明はそれに限定されるものではない。例えば、コンテンツを複数のブロックに分割したうちのいくつかのブロックを第1のコンテンツ鍵（CK1）で暗号化し、他のブロックを第2のコンテンツ鍵（CK2）で暗号化するようにしてもよい。

【0169】

なお、本実施の形態は、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものであるが、本発明はそれに限定されるものではない。前記した実施の形態2のように、鍵生成装置で各カテゴリ用の暗号化メディア鍵データ及び暗号化コンテンツ鍵を生成して記録媒体に記録し、記録装置で暗号化メディア鍵データ及び暗号化コンテンツ鍵を復号してコンテンツを暗号化する構成とすることにより、書き換え型もしくは追記型の記録媒体を用いるシステムにも適用することができる。

【0170】

（実施の形態6）

本発明の実施の形態6は、実施の形態1と同様、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものである。

【0171】

以下、本発明の実施の形態6について、図面を参照にしながら説明する。図31は、コンテンツを暗号化して記録する記録装置3100及び記録媒体3120を示しており、図32は、記録媒体3120から暗号化コンテンツを読み出して復号する第1の再生装置3200を示しており、図33は、記録媒体3120から暗号化コンテンツを読み出して復号する第2の再生装置3300を示している。また、図34は記録媒体3120に記録される各種データ的具体例を示している。

【0172】

図31の記録装置3100が図1の記録装置100と異なる点は、コンテンツ鍵生成部3109で外部から入力される第1及び第2のシードを用いてコンテンツ鍵を生成し、メディア鍵を用いて第1及び第2のシードをそれぞれ第1のシード暗号化部3107及び第2のシード暗号化部3108で暗号化して、記録媒体3120に記録するようにしたことである。その他の点は図1の記録装置100と同じであるので、その説明は省略する。

【0173】

記録媒体3120は、第1の暗号化メディア鍵データを記録する第1の暗号化メディア鍵データ記録領域3121と、第2の暗号化メディア鍵データを記録する第2の暗号化メディア鍵データ記録領域3122と、第1のシード暗号化部3107が生成した第1の暗号化シードを記録する第1の暗号化シード記録領域3123と、第2のシード暗号化部3

108が生成した第2の暗号化シードを記録する第2の暗号化シード記録領域3124と、暗号化コンテンツを記録する暗号化コンテンツ記録領域3125とを備える。

【0174】

第1の再生装置3200は、読み出し装置3210及び復号装置3220とから構成される。

【0175】

読み出し装置3210は、デバイス鍵を秘密に保有するデバイス鍵格納部3211と、デバイス鍵を用いて記録媒体3120から読み出した第2の暗号化メディア鍵データを復号してメディア鍵を取得する第2のメディア鍵復号部3212と、取得したメディア鍵を用いて記録媒体から読み出した第2の暗号化シードを復号して第2のシードを取得する第2のシード復号部3213と、取得した第2のシードを、記録媒体3220から読み出した第1の暗号化メディア鍵データ、第1の暗号化シード、及び暗号化コンテンツとともに復号装置3220に供給する。本実施の形態において、読み出し装置3210は上記した構成要素がハードウェアで実装されており、第2のカテゴリに属するものとした。

【0176】

復号装置3220は、デバイス鍵を秘密に保有するデバイス鍵格納部3221と、デバイス鍵を用いて読み出し装置3210から供給される第1の暗号化メディア鍵データを復号してメディア鍵を取得する第1のメディア鍵復号部3222と、取得したメディア鍵を用いて読み出し装置3210から供給される第1の暗号化シードを復号して第1のシードを取得する第1のシード復号部3223と、取得した第1のシードと読み出し装置3210から供給される第2のシードを用いてコンテンツ鍵を生成するコンテンツ鍵生成部3224と、生成したコンテンツ鍵を用いて読み取り装置3210から供給される暗号化コンテンツを復号するコンテンツ復号部3225とを備える。本実施の形態において、復号装置3220は上記した構成要素がソフトウェアで実装されており、第1のカテゴリに属するものとした。

【0177】

第2の再生装置3300は、第2のカテゴリの再生装置であり、デバイス鍵を秘密に保有するデバイス鍵格納部3301と、デバイス鍵を用いて記録媒体3120から読み出した第2の暗号化メディア鍵データを復号してメディア鍵を取得するメディア鍵復号部3302と、取得したメディア鍵を用いて記録媒体から読み出した第1の暗号化シードを復号して第1のシードを取得する第1のシード復号部3303と、取得したメディア鍵を用いて記録媒体3120から読み出した第2の暗号化シードを復号して第2のシードを取得する第2のシード復号部3304と、取得した第1のシードと第2のシードからコンテンツ鍵を生成するコンテンツ鍵生成部3305と、生成したコンテンツ鍵を用いて記録媒体3120から読み出した暗号化コンテンツを復号するコンテンツ復号部3306とを備える。本実施の形態において、第2の再生装置3300は上記した構成要素がハードウェアで実装されており、第2のカテゴリに属するものとした。

【0178】

本実施の形態ではパソコン上のアプリケーションプログラムのようにソフトウェアで実装される復号装置を第1のカテゴリに属する復号装置とし、一般的な民生プレーヤ及びパソコンに接続もしくは内蔵される光ディスクドライブのようにハードウェアで実装される装置を第2のカテゴリに属する装置とした。

【0179】

図34は、m台の第1のカテゴリの復号装置及びn台の第2のカテゴリの装置がそれぞれ固有のデバイス鍵を1個だけ保有しており、第1のカテゴリの復号装置2と第2のカテゴリの装置3が無効化されているとした場合の、記録媒体3120に記録される各種データの具体例を示している。図34中で、第1のカテゴリの復号装置i ($i=1\sim m$) が保有するデバイス鍵をDKA_i、第2のカテゴリの装置j ($j=1\sim n$) が保有するデバイス鍵をDKA_jとしている。また、E_a(X, Y)、E_b(X, Y)、E_c(X, Y)、E_d(X, Y)、及びE_e(X, Y)はデータYを鍵データXを用いて暗号化する関数を

意味する。なお、使用される暗号アルゴリズムは公知の技術で実現可能であり、本実施の形態では鍵長 56 ビットの DES 暗号を使用した。

【0180】

第1の暗号化メディア鍵データ記録領域 3121 及び第2の暗号化メディア鍵データ記録領域 3122 に記録されるデータは、それぞれ、前記した実施の形態1における第1の暗号化メディア鍵データ記録領域 121 及び第2の暗号化メディア鍵データ記録領域 122 に記録されるデータと同じであるので、その説明は省略する。

【0181】

(第1の暗号化シード記録領域 3123)

第1の暗号化シード記録領域 3123 にはメディア鍵 (MK) で暗号化された第1のシード (SD1) が記録されている。

【0182】

(第2の暗号化シード記録領域 3124)

第2の暗号化シード記録領域 3124 にはメディア鍵 (MK) で暗号化された第2のシード (SD2) が記録されている。

【0183】

(暗号化コンテンツ記録領域 3125)

暗号化コンテンツ記録領域 3125 には、コンテンツ鍵 (CK) で暗号化されたコンテンツが記録されている。

【0184】

以上のように構成された本発明の実施の形態において、例えば第1のカテゴリの復号装置に付与したデバイス鍵の多数や、第1の暗号化メディア鍵データを復号するアルゴリズムがインターネット上で不正に公開され、第1のカテゴリの復号装置の無効化が機能しなくなったと判断された場合には、第1のカテゴリの復号装置の無効化システムを更新することになる。以下、その具体例を説明する。

【0185】

(システム更新の具体例1)

第1のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体 3120 に記録する各種データの具体例1を図35に示す。図34との違いは、第1の暗号化メディア鍵データの生成に用いるデバイス鍵を DKA1 ~ DKA_m から DKA'1 ~ DKA'm に変更したことである。これは、前記した実施の形態1で述べたシステム更新の具体例1と同様であるので、詳細についての説明は省略する。

【0186】

ここで、新たなデバイス鍵 (DKA'1 ~ DKA'm) のうちの各デバイス鍵は、システム更新前のデバイス鍵 (DKA1 ~ DKA_m) のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵が DKA2 以外に存在したとしても、そのデバイス鍵を使って図35の記録媒体から読み出した第1の暗号化メディア鍵データを復号してメディア鍵 (MK) を取得することはできず、コンテンツを再生することはできない。

【0187】

なお、上記したシステム更新に際して、第2の暗号化メディア鍵データの生成に用いるデバイス鍵 (DKB1 ~ DKB_n) は変更されていないので、第2のカテゴリに属する装置には何らの変更を加える必要がない。

【0188】

(システム更新の具体例2)

第1のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体 3120 に記録する各種データの具体例2を図36に示す。図34との違いは、第1の暗号化メディア鍵データの生成に用いるデバイス鍵を DKA1 ~ DKA_m から DKA'1 ~ DKA'm に変更したことと、暗号化アルゴリズムを E_a(X, Y) から E_{a'}(X, Y) に変更したことである。これは、前記した実施の形態1で述べたシステム

更新の具体例 2 と同様であるので、詳細についての説明は省略する。

【0189】

ここで、新たなデバイス鍵 ($DKA' 1 \sim DKA' m$) のうちの各デバイス鍵は、システム更新前のデバイス鍵 ($DKA 1 \sim DKA m$) のどれとも一致しないようになっているので、システム更新前に不正な解析行為により暴露されたデバイス鍵が $DKA 2$ 以外に存在したとしても、そのデバイス鍵を使って図 36 の記録媒体から読み出した第 1 の暗号化メディア鍵データを復号してメディア鍵 (MK) を取得することはできず、コンテンツを再生することはできない。

【0190】

また、デバイス鍵の鍵長や暗号アルゴリズムを変更して暗号強度の高いものにすることができ、システムを解析してデバイス鍵を不正取得するといった行為を困難にすることができる。

【0191】

なお、上記したシステム更新に際して、第 2 の暗号化メディア鍵データの生成に用いるデバイス鍵 ($DKB 1 \sim DKB n$) 及び第 2 の暗号化メディア鍵データの暗号化アルゴリズムは変更されていないので、第 2 のカテゴリに属する装置には何らの変更を加える必要がない。

【0192】

以上のように構成された本発明の実施の形態 5 によれば、第 1 のカテゴリの装置 (復号装置 3220) 及び第 2 のカテゴリの装置 (読み出し装置 3210 及び第 2 の再生装置 3300) は、それぞれ異なるカテゴリの装置を無効化するための第 1 もしくは第 2 の暗号化メディア鍵データを読み込む必要がないため、装置内に設けるメモリ容量を小さくでき、処理時間も短くできる。また、第 1 の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムを第 2 の暗号化メディア鍵データの生成に用いる暗号化アルゴリズムと異なるものとすることができるため、第 1 のカテゴリの復号装置の無効化システムが暴露されるような事態に陥った場合にも、第 1 のカテゴリの復号装置に付与するデバイス鍵の鍵長や第 1 の暗号化メディア鍵データの生成アルゴリズムを変更することで、第 2 のカテゴリの装置に影響を与えることなく、無効化システムを変更することが可能になる。さらに、第 1 のカテゴリの復号装置 3220 には、第 2 の暗号化シードを復号するためのアルゴリズムは実装されていないので、第 1 のカテゴリの復号装置の何れかを解析して保有するデバイス鍵や復号アルゴリズムを暴露したとしても、コンテンツ毎に異なる第 2 の暗号化シードを復号することはできず、第 1 のカテゴリに対する不正行為がシステム全体に影響することを防ぐことができ、より堅牢な著作権保護システムを構築できる。これは、本実施の形態のように第 1 のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される復号装置とし、第 2 のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される再生装置もしくは読み取り装置とした場合に、特に有効である。

【0193】

なお、図 31 で、メディア鍵、第 1 のシード、及び第 2 のシードが記録装置 3100 の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、記録装置 3100 がメディア鍵、第 1 のシード、及び第 2 のシードを格納する格納部を有する構成であってもよい。また、記録装置 3100 がメディア鍵、第 1 のシード、及び第 2 のシードをその都度生成する生成部を有する構成であってもよい。

【0194】

また、図 31 では、第 1 のシード及び第 2 のシードからコンテンツ鍵を生成し、コンテンツをコンテンツ鍵で暗号化し、第 1 及び第 2 のシードをメディア鍵で暗号化する構成としたが、本発明はそれに限定されるものではない。例えば、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

【0195】

また、本実施の形態では記録装置として図 31 に示すように、各カテゴリのデバイス鍵

格納部、メディア鍵暗号化部、シード暗号化部、コンテンツ鍵生成部、コンテンツ暗号化部及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではなく、記録装置が分離して構成されるものであっても良い。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、シード暗号化部、及びコンテンツ鍵生成部（図 31 中の破線で囲んだ部分）は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置される装置に内蔵され、コンテンツ暗号部や記録媒体に各データへの記録はコンテンツ製造機関や記録媒体製造機関に設置される装置で実行される形態であっても良い。

【0196】

また、本実施の形態ではシステム更新において第 1 の暗号化メディア鍵データを生成する際に、図 35 の E a (DKA' 2, 0) や図 36 の E a' (DKA' 2, 0) のようにシステム更新の時点で無効化されている復号装置にもデータを割り当てる構成としているが、無効化されている復号装置にはデータを割り当てない構成とすることも可能である。その場合、無効化されていない復号装置の使うべき暗号化メディア鍵の位置も更新し、新たなデバイス鍵を付与する際に新たな位置情報も付与することで、システム更新の前後において暗号化メディア鍵の位置が変わったとしても無効化されていない復号装置は適切なデータを用いることができ、正しいメディア鍵を得ることができる。こうした場合、システム更新後の第 1 の暗号化メディア鍵データ記録領域に格納すべきデータの容量を削減することができる。あるいは容量の最大値が限定されている場合は新たに第 1 のカテゴリに属する復号装置の台数を増やすことが可能となる。

【0197】

また、本実施の形態では、図 34 に示すような暗号化メディア鍵データを用いて復号装置の無効化を行う方法としたが、無効化の方法は他の方法を利用してもよく、例えば特許文献 1 として開示されている本構造を利用した無効化方法を用いても良い。

【0198】

また、本実施の形態では、暗号アルゴリズムとして鍵長 56 bit の DES、あるいはシステム更新後の暗号アルゴリズムとして鍵長 112 bit の 2 キートリプル DES を用いたが、本発明はこれに限定されるものではなく、他の暗号アルゴリズム、例えば次世代の標準暗号とされる鍵長 128 bit の AES 等を用いても良い。

【0199】

なお、本実施の形態は、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものであるが、本発明はそれに限定されるものではない。前記した実施の形態 2 のように、鍵生成装置で各カテゴリ用の暗号化メディア鍵データ及び暗号化シードを生成して記録媒体に記録し、記録装置で暗号化メディア鍵データ及び暗号化シードを復号し、コンテンツ鍵を生成し、コンテンツを暗号化する構成とすることにより、書き換え型もしくは追記型の記録媒体を用いるシステムにも適用することができる。

【0200】

(実施の形態 7)

本発明の実施の形態 7 は、実施の形態 6 のシステムにおいて、第 1 のカテゴリと第 2 のカテゴリに対して個別にメディア鍵を設け、それぞれを用いた第 1 の暗号化シードの階層を設けるようにしたものである。

【0201】

以下、本発明の実施の形態 7 について、図面を参照しながら説明する。図 37 は、コンテンツを暗号化して記録する記録装置 3700 及び記録媒体 3720 を示しており、図 38 は、記録媒体 3720 から暗号化コンテンツを読み出して復号する第 1 の再生装置 3800 を示しており、図 39 は、記録媒体 3720 から暗号化コンテンツを読み出して復号する第 2 の再生装置 3900 を示している。また、図 40 は記録媒体 3720 に記録される各種データの具体例を示している。

【0202】

図37の記録装置3700が図31の記録装置3100と異なる点は、第1のカテゴリに対しては第1のメディア鍵を、第2のカテゴリに対しては第2のメディア鍵を、個別に設け、第1及び第2のメディア鍵をそれぞれ第1のメディア鍵暗号化部3705及び第2のメディア鍵暗号化部3706で暗号化し、第1のシードを第1及び第2のメディア鍵を用いてそれぞれ第1シード暗号化部(1)3707及び第1のシード暗号化部(2)3711で暗号化し、記録媒体3720に記録するようにしたことである。その他の点については、前記した実施の形態6の記録装置3100と同じであるので、その説明は省略する。

【0203】

記録媒体3720は、第1の暗号化メディア鍵データを記録する第1の暗号化メディア鍵データ記録領域3721と、第2の暗号化メディア鍵データを記録する第2の暗号化メディア鍵データ記録領域3722と、第1のシード暗号化部(1)3707が生成した第1の暗号化シード(1)を記録する第1の暗号化シード(1)記録領域3723と、第1のシード暗号化部(2)3711が生成した第1の暗号化シード(2)を記録する第1の暗号化シード(2)記録領域3726と、第2の暗号化シードを記録する第2の暗号化シードデータ記録領域3724と、暗号化コンテンツを記録する暗号化コンテンツ記録領域3725とを備える。

【0204】

第1の再生装置3800において復号装置3820は、読み出し装置3810が記録媒体3720から読み出した第1の暗号化シード(1)を復号して第1のシードを取得する。その他の点については、前記した実施の形態6における第1の再生装置3200と同様であるので、その説明は省略する。

【0205】

第2の再生装置3900は、記録媒体3720から読み出した第1の暗号化シード(2)を復号して第1のシードを取得する。その他の点については、前記した実施の形態6における第2の再生装置3300と同様であるので、その説明は省略する。

【0206】

図40は、記録媒体3720に記録される各種データの具体例を示している。第1の暗号化メディア鍵データ記録領域3721には、第1のカテゴリの復号装置が保有するデバイス鍵(DKA1~DKAm)で暗号化された第1のメディア鍵(MK1)が記録されており、第2の暗号化メディア鍵データ記録領域3722には、第2のカテゴリの装置が保有するデバイス鍵(DKB1~DKBm)で暗号化された第2のメディア鍵(MK2)がきろくされている。また、第1の暗号化シードデータ(1)記録領域3723には、第1のメディア鍵(MK1)で暗号化された第1のシード(SD1)が記録されており、第1の暗号化シードデータ(2)記録領域3726には、第2のメディア鍵(MK2)で暗号化された第1のシード(SD1)が記録されている。その他の点については、前記した図34と同じであるので、説明を省略する。なお、図40中の、Ef(X, Y)はデータYを鍵データXを用いて暗号化する関数を意味し、本実施の形態では鍵長56ビットのDES暗号を使用した。

【0207】

以上のように構成された本発明の実施の形態7において、例えば第1のカテゴリの復号装置に付与したデバイス鍵の多数や、第1の暗号化メディア鍵データを復号するアルゴリズムがインターネット上で不正に公開され、第1のカテゴリの復号装置の無効化が機能しなくなったと判断された場合には、第1のカテゴリの復号装置の無効化システムを更新することになる。以下、その具体例を説明する。

【0208】

(システム更新の具体例1)

第1のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体3720に記録する各種データの具体例1を図41に示す。図40との違いは、第1の暗号化メディア鍵データの生成に用いるデバイス鍵をDKA1~DKAmから

DKA' 1 ~ DKA' mに変更したことである。これは、前記した実施の形態1で述べたシステム更新の具体例1と同様であるので、詳細についての説明は省略する。

【0209】

(システム更新の具体例2)

第1のカテゴリの復号装置の無効化が機能しなくなったと判断されて以降、新たに作成する記録媒体3720に記録する各種データの具体例2を図42に示す。図40との違いは、第1の暗号化メディア鍵データの生成に用いるデバイス鍵をDKA1 ~ DKA mからDKA' 1 ~ DKA' mに変更したこと、暗号化アルゴリズムをEa (X, Y) からEa' (X, Y)に変更したこと、及び第1の暗号化シード(1)の暗号化アルゴリズムをEc (X, Y) からEc' (X, Y)に変更したことである。これは、前記した実施の形態3で述べたシステム更新の具体例2と同様であるので、詳細についての説明は省略する。

【0210】

以上のように構成された本発明の実施の形態7によれば、前記した実施の形態6同様に、堅牢な著作権保護システムを構築できる。さらに、本実施の形態では第1のカテゴリと第2のカテゴリに対して個別にメディア鍵を設け、それぞれを用いた暗号化シードの階層を設けることにより、カテゴリ間の独立性を高めることが可能となる。すなわち第1のカテゴリに属する装置からデバイス鍵が暴露された場合であっても、それを用いて得られるメディア鍵は第1のメディア鍵のみであり、第2のメディア鍵が暴露されることを防ぐことが可能となる。これは、本実施の形態のように第1のカテゴリは復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される復号装置とし、第2のカテゴリは堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される再生装置もしくは読み取り装置とした場合に、特に有効である。

なお、図37で、第1のメディア鍵、第2のメディア鍵、第1のシード、及び第2のシードが記録装置3700の外部から入力される形態としたが、本発明はその構成に限定されるものではない。例えば、記録装置3700がこれらを格納する格納部を有する構成であってもよい。また、記録装置3700がこれらをその都度生成する生成部を有する構成であってもよい。

【0211】

また、図37では、第1のシード及び第2のシードからコンテンツ鍵を生成し、コンテンツをコンテンツ鍵で暗号化し、第1及び第2のシードをメディア鍵で暗号化する構成としたが、本発明はそれに限定されるものではない。例えば、鍵を追加して暗号化の階層をさらに増やす構成であってもよい。

【0212】

また、本実施の形態では記録装置として図37に示すように、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、シード暗号化部、コンテンツ鍵生成部、コンテンツ暗号化部及び記録媒体への各データの記録が一体の構成としたが、本発明はそれに限定されるものではなく、記録装置が分離して構成されるものであっても良い。例えば、各カテゴリのデバイス鍵格納部、メディア鍵暗号化部、シード暗号化部、及びコンテンツ鍵生成部(図37中の破線で囲んだ部分)は、その管理、運用に高い秘匿性が要求されることから、システム全体の鍵管理や再生装置に対する鍵発行等を運用する機関に設置される装置に内蔵され、コンテンツ暗号部や記録媒体に各データへの記録はコンテンツ製造機関や記録媒体製造機関に設置される装置で実行される形態であっても良い。

【0213】

また、本実施の形態ではシステム更新において第1の暗号化メディア鍵データを生成する際に、図41のEa (DKA' 2, 0)や図42のEa' (DKA' 2, 0)のようにシステム更新の時点で無効化されている復号装置にもデータを割り当てる構成としているが、無効化されている復号装置にはデータを割り当てない構成とすることも可能である。その場合、無効化されていない復号装置の使うべき暗号化メディア鍵の位置も更新し、新たなデバイス鍵を付与する際に新たな位置情報も付与することで、システム更新の前後において暗号化メディア鍵の位置が変わったとしても無効化されていない復号装置は適切な

データを用いることができ、正しいメディア鍵を得ることができる。こうした場合、システム更新後の第1の暗号化メディア鍵データ記録領域に格納すべきデータの容量を削減することができる。あるいは容量の最大値が限定されている場合は新たに第1のカテゴリに属する復号装置の台数を増やすことが可能となる。

【0214】

また、本実施の形態では、図40に示すような暗号化メディア鍵データを用いて復号装置の無効化を行う方法としたが、無効化の方法は他の方法を利用してもよく、例えば特許文献1として開示されている木構造を利用した無効化方法を用いても良い。

【0215】

また、本実施の形態では、暗号アルゴリズムとして鍵長56bitのDES、あるいはシステム更新後の暗号アルゴリズムとして鍵長112bitの2キートリプルDESを用いたが、本発明はこれに限定されるものではなく、他の暗号アルゴリズム、例えば次世代の標準暗号とされる鍵長128bitのAES等を用いても良い。

【0216】

なお、本実施の形態は、再生専用の記録媒体を用いてコンテンツを配布し、再生装置でコンテンツを再生するシステムに本発明を適用したものであるが、本発明はそれに限定されるものではない。前記した実施の形態2のように、鍵生成装置で各カテゴリ用の暗号化メディア鍵データ及び暗号化シードを生成して記録媒体に記録し、記録装置で暗号化メディア鍵データ及び暗号化シードを復号し、コンテンツ鍵を生成し、コンテンツを暗号化する構成とすることにより、書き換え型もしくは追記型の記録媒体を用いるシステムにも適用することができる。

【産業上の利用可能性】

【0217】

本発明にかかる著作権保護システムは、装置内に設けるメモリのサイズを小さくでき、かつ、あるカテゴリの装置が不正に解析されてアルゴリズムや多数の鍵が暴露された場合にも、そのカテゴリの装置用の暗号化・復号のアルゴリズムや鍵長を変更することで、他のカテゴリの装置に何らの変更を加えることなく、システム全体の無効化機能を維持できるという効果があり、著作物をデジタル化したコンテンツを光ディスク等の大容量記録媒体に記録もしくは再生するシステムにおいて、復号アルゴリズムや鍵の更新や追加が容易ではあるが堅牢な実装が困難なソフトウェアで実装される記録装置もしくは再生装置と、堅牢ではあるが復号アルゴリズムや鍵の更新や追加が困難なハードウェアで実装される記録装置もしくは再生装置とが存在するような場合に有用である。

【図面の簡単な説明】

【0218】

【図1】本発明の実施の形態1における記録装置及び記録媒体を示すブロック図

【図2】本発明の実施の形態1における記録媒体及び第1のカテゴリの再生装置を示すブロック図

【図3】本発明の実施の形態1における記録媒体及び第2のカテゴリの再生装置を示すブロック図

【図4】本発明の実施の形態1における記録媒体に記録するデータの具体例を示す模式図

【図5】本発明の実施の形態1におけるシステム更新の具体例1を示す模式図

【図6】本発明の実施の形態1におけるシステム更新の具体例2を示す模式図

【図7】本発明の実施の形態2における鍵生成装置及び記録媒体を示すブロック図

【図8】本発明の実施の形態2における第1のカテゴリの記録装置及び記録媒体を示すブロック図

【図9】本発明の実施の形態2における第2のカテゴリの記録装置及び記録媒体を示すブロック図

【図10】本発明の実施の形態2における記録媒体及び第1のカテゴリの再生装置を示すブロック図

【図 1 1】本発明の実施の形態 2 における記録媒体及び第 2 のカテゴリの再生装置を示すブロック図

【図 1 2】本発明の実施の形態 2 における記録媒体に記録するデータの具体例を示す模式図

【図 1 3】本発明の実施の形態 3 における記録装置及び記録媒体を示すブロック図

【図 1 4】本発明の実施の形態 3 における記録媒体及び第 1 のカテゴリの再生装置を示すブロック図

【図 1 5】本発明の実施の形態 3 における記録媒体及び第 2 の再生装置を示すブロック図

【図 1 6】本発明の実施の形態 3 における記録媒体に記録するデータの具体例を示す模式図

【図 1 7】本発明の実施の形態 3 におけるシステム更新の具体例 1 を示す模式図

【図 1 8】本発明の実施の形態 3 におけるシステム更新の具体例 2 を示す模式図

【図 1 9】本発明の実施の形態 4 における記録装置及び記録媒体を示すブロック図

【図 2 0】本発明の実施の形態 4 における記録媒体及び第 1 の再生装置を示すブロック図

【図 2 1】本発明の実施の形態 4 における記録媒体及び第 2 の再生装置を示すブロック図

【図 2 2】本発明の実施の形態 4 における記録媒体に記録するデータの具体例を示す模式図

【図 2 3】本発明の実施の形態 4 におけるシステム更新の具体例 1 を示す模式図

【図 2 4】本発明の実施の形態 4 におけるシステム更新の具体例 2 を示す模式図

【図 2 5】本発明の実施の形態 5 における記録装置及び記録媒体を示すブロック図

【図 2 6】本発明の実施の形態 5 における記録媒体及び第 1 の再生装置を示すブロック図

【図 2 7】本発明の実施の形態 5 における記録媒体及び第 2 の再生装置を示すブロック図

【図 2 8】本発明の実施の形態 5 における記録媒体に記録するデータの具体例を示す模式図

【図 2 9】本発明の実施の形態 5 におけるシステム更新の具体例 1 を示す模式図

【図 3 0】本発明の実施の形態 5 におけるシステム更新の具体例 2 を示す模式図

【図 3 1】本発明の実施の形態 6 における記録装置及び記録媒体を示すブロック図

【図 3 2】本発明の実施の形態 6 における記録媒体及び第 1 の再生装置を示すブロック図

【図 3 3】本発明の実施の形態 6 における記録媒体及び第 2 の再生装置を示すブロック図

【図 3 4】本発明の実施の形態 6 における記録媒体に記録するデータの具体例を示す模式図

【図 3 5】本発明の実施の形態 6 におけるシステム更新の具体例 1 を示す模式図

【図 3 6】本発明の実施の形態 6 におけるシステム更新の具体例 2 を示す模式図

【図 3 7】本発明の実施の形態 7 における記録装置及び記録媒体を示すブロック図

【図 3 8】本発明の実施の形態 7 における記録媒体及び第 1 の再生装置を示すブロック図

【図 3 9】本発明の実施の形態 7 における記録媒体及び第 2 の再生装置を示すブロック図

【図 4 0】本発明の実施の形態 7 における記録媒体に記録するデータの具体例を示す模式図

【図 4 1】本発明の実施の形態 7 におけるシステム更新の具体例 1 を示す模式図

【図 4 2】本発明の実施の形態 7 におけるシステム更新の具体例 2 を示す模式図

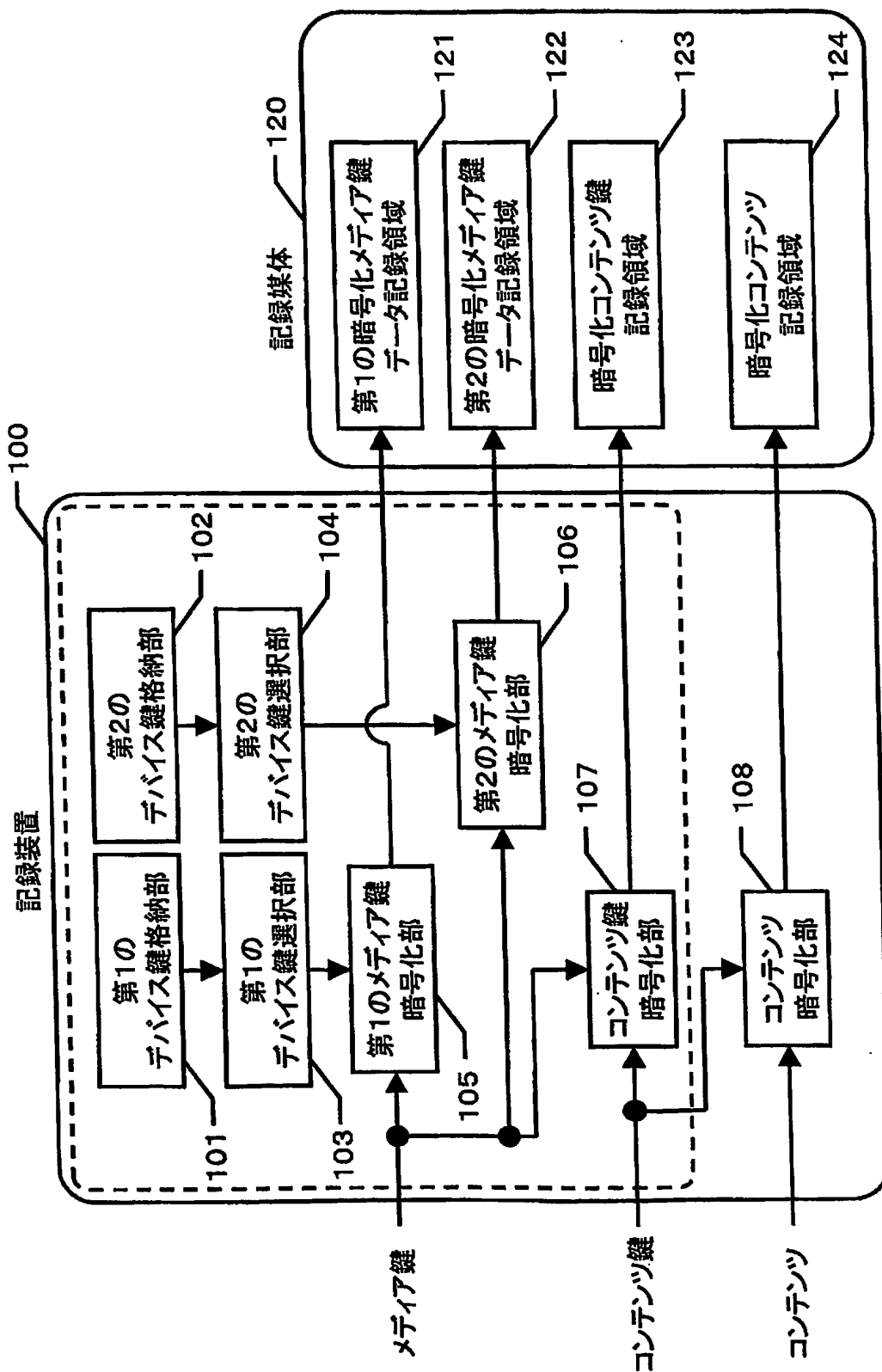
【符号の説明】

【0219】

- 100 記録装置
- 101 第1のデバイス鍵格納部
- 102 第2のデバイス鍵格納部
- 103 第1のデバイス鍵選択部
- 104 第2のデバイス鍵選択部
- 105 第1のメディア鍵暗号化部
- 106 第2のメディア鍵暗号化部
- 107 コンテンツ鍵暗号化部
- 108 コンテンツ暗号化部
- 120 記録媒体
- 121 第1の暗号化メディア鍵データ記録領域
- 122 第2の暗号化メディア鍵データ記録領域
- 123 暗号化コンテンツ鍵データ記録領域
- 124 暗号化コンテンツ記録領域

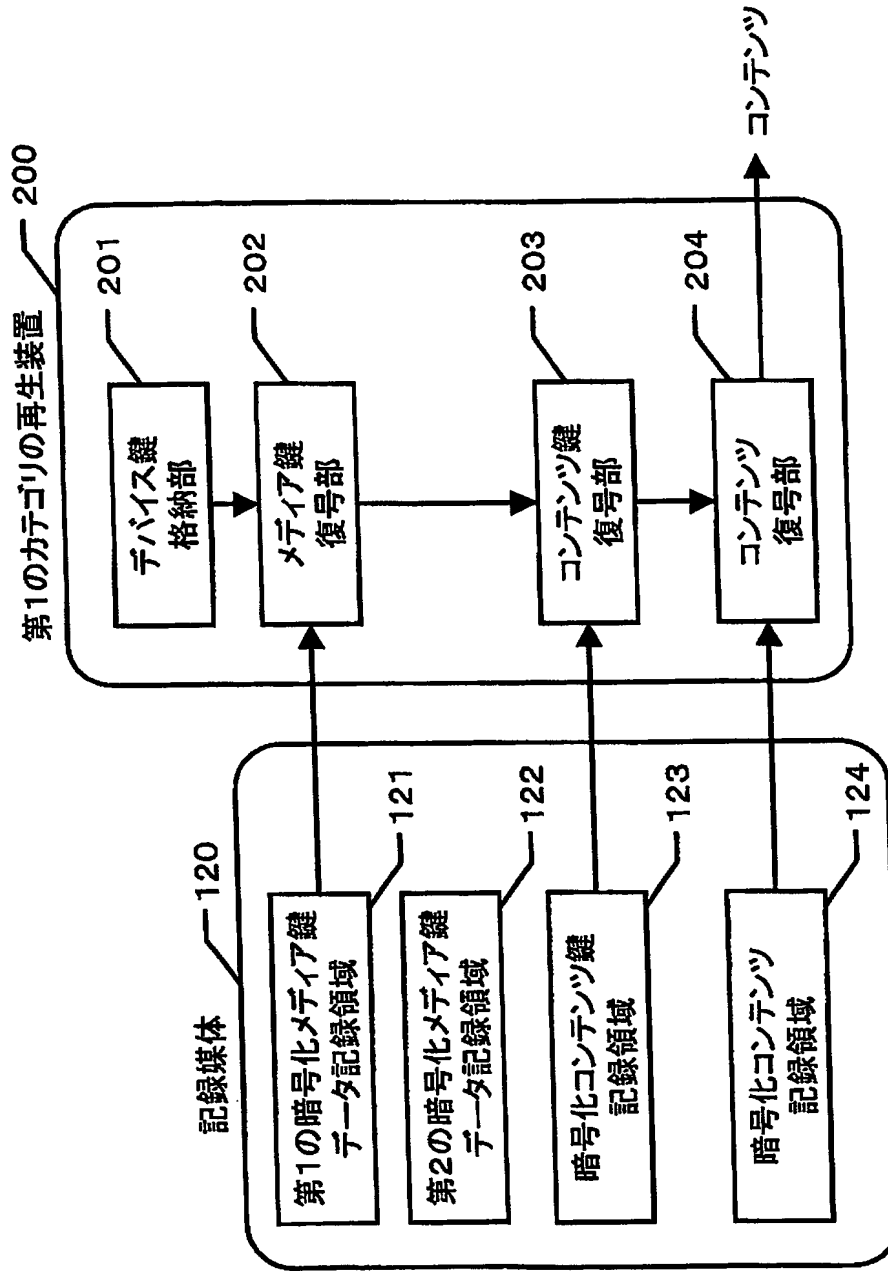
【書類名】 図面
【図 1】

本発明の実施の形態 1 における記録装置及び記録媒体



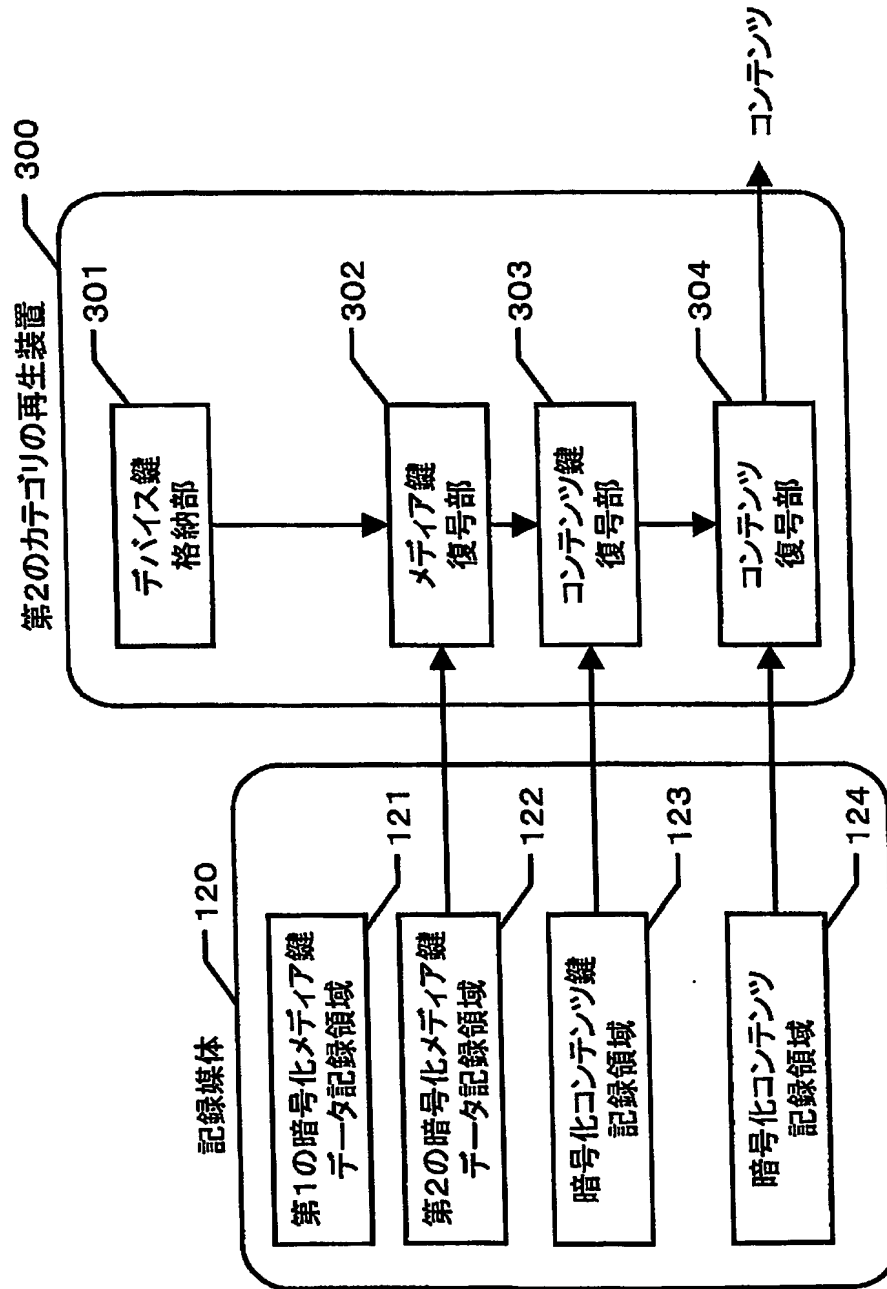
【図 2】

本発明の実施の形態 1 における記録媒体及び第 1 のカテゴリの再生装置



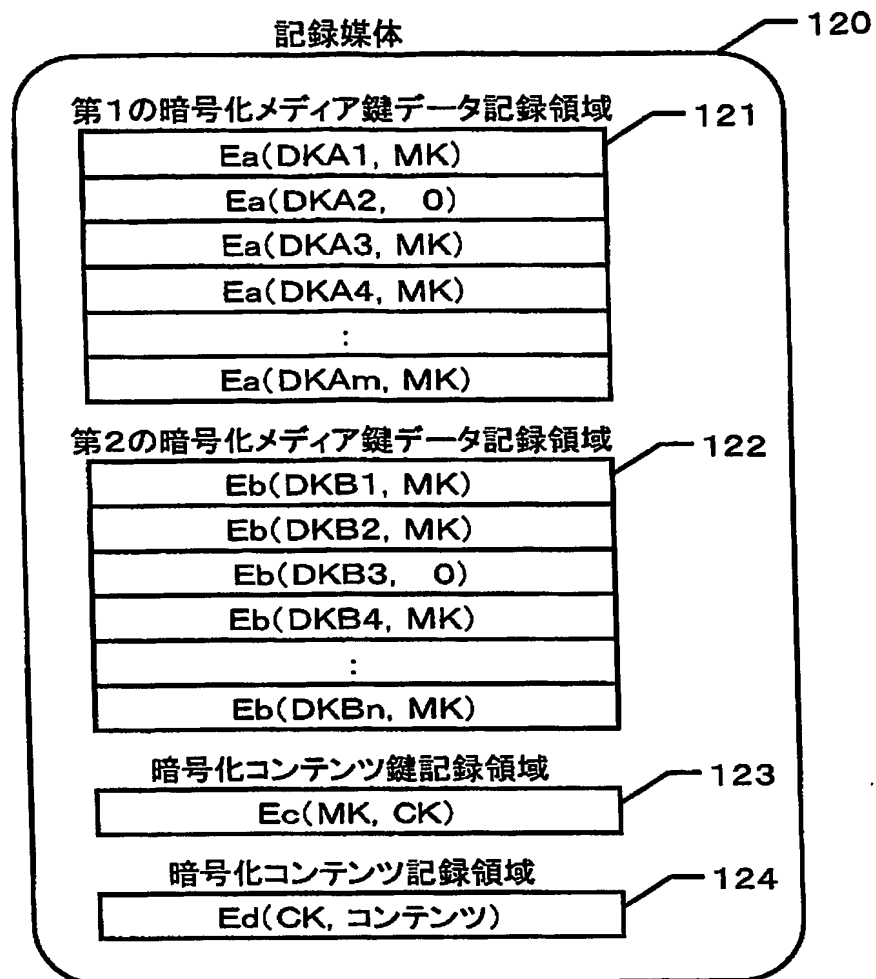
【図3】

本発明の実施の形態1における記録媒体及び第2のカテゴリの再生装置



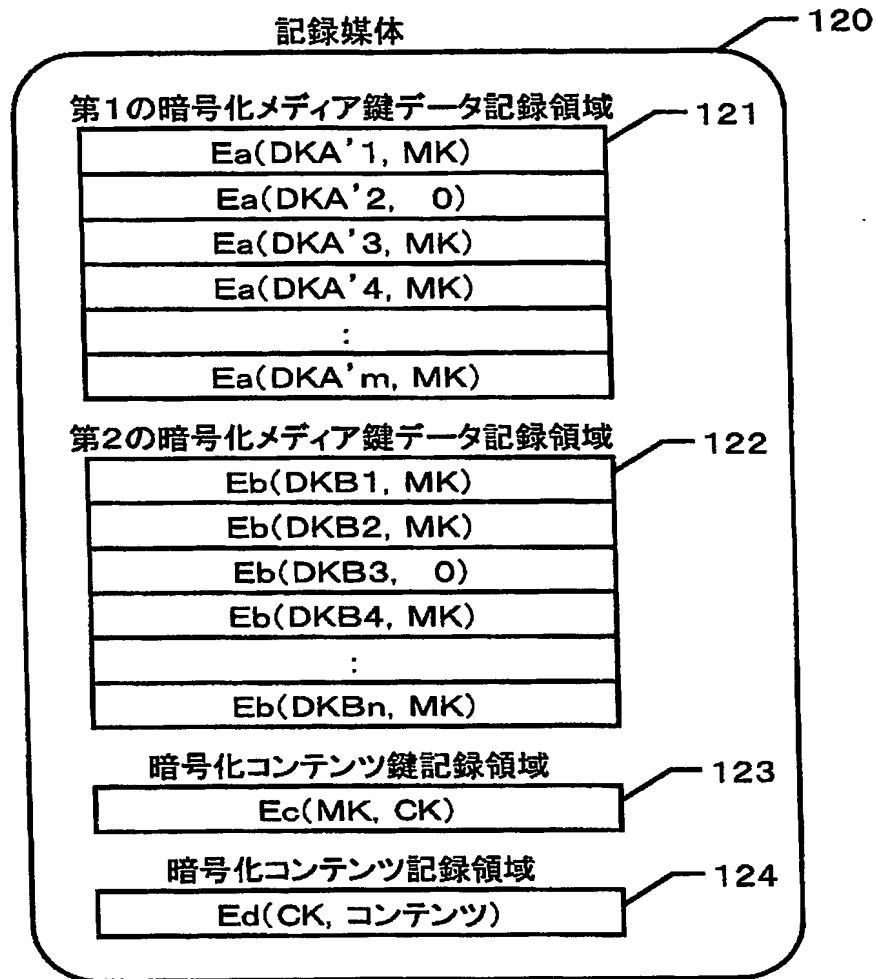
【図4】

本発明の実施の形態1における記録媒体に記録するデータの具体例



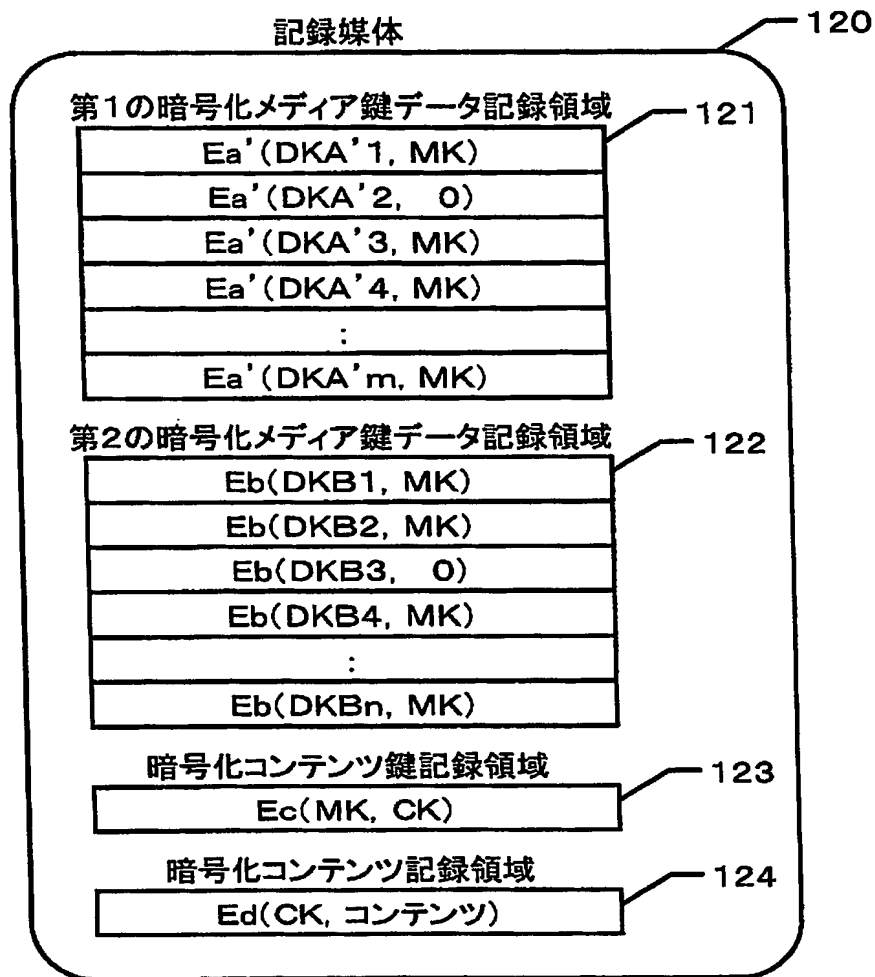
【図5】

本発明の実施の形態1におけるシステム更新の具体例1



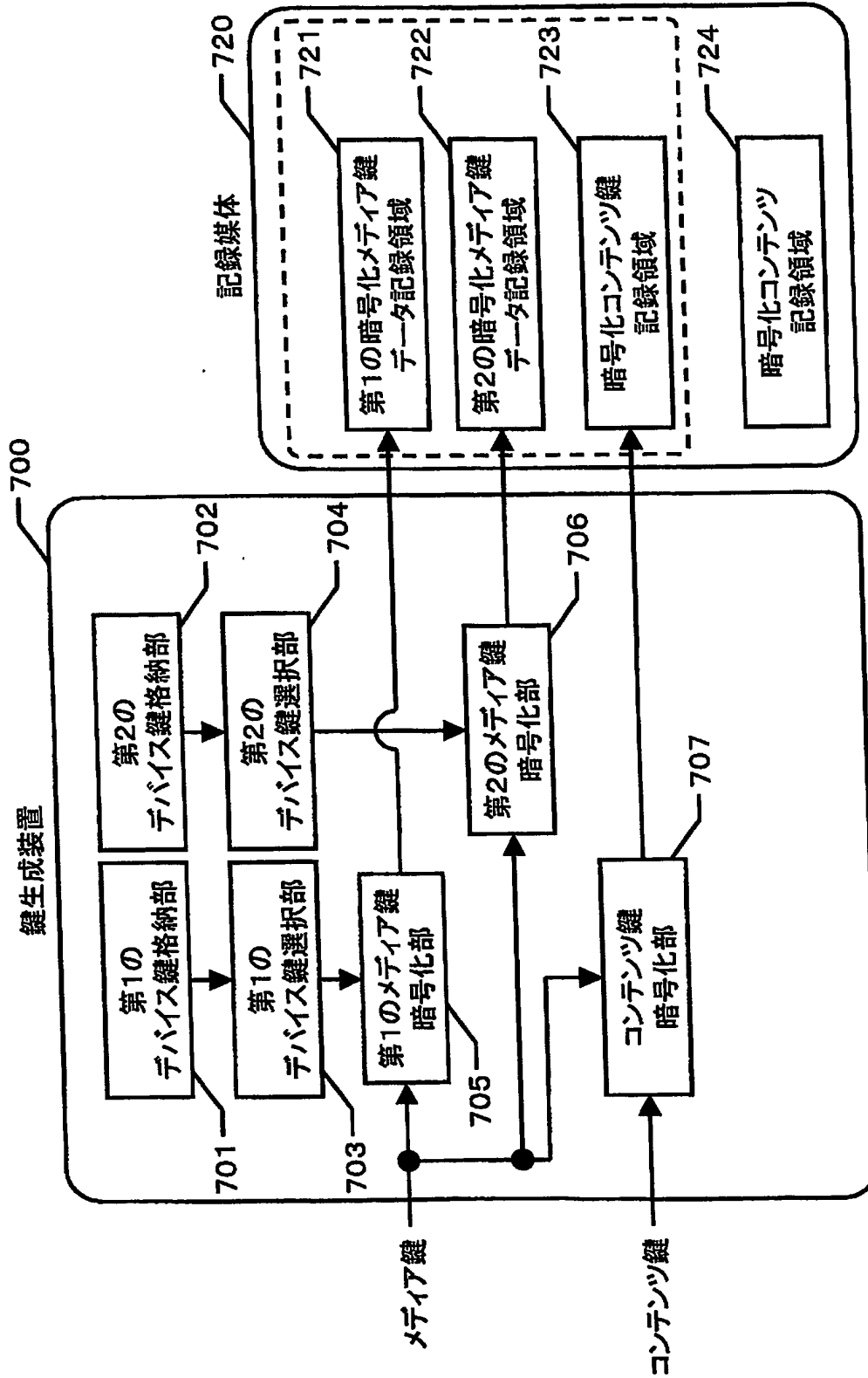
【図6】

本発明の実施の形態1におけるシステム更新の具体例2



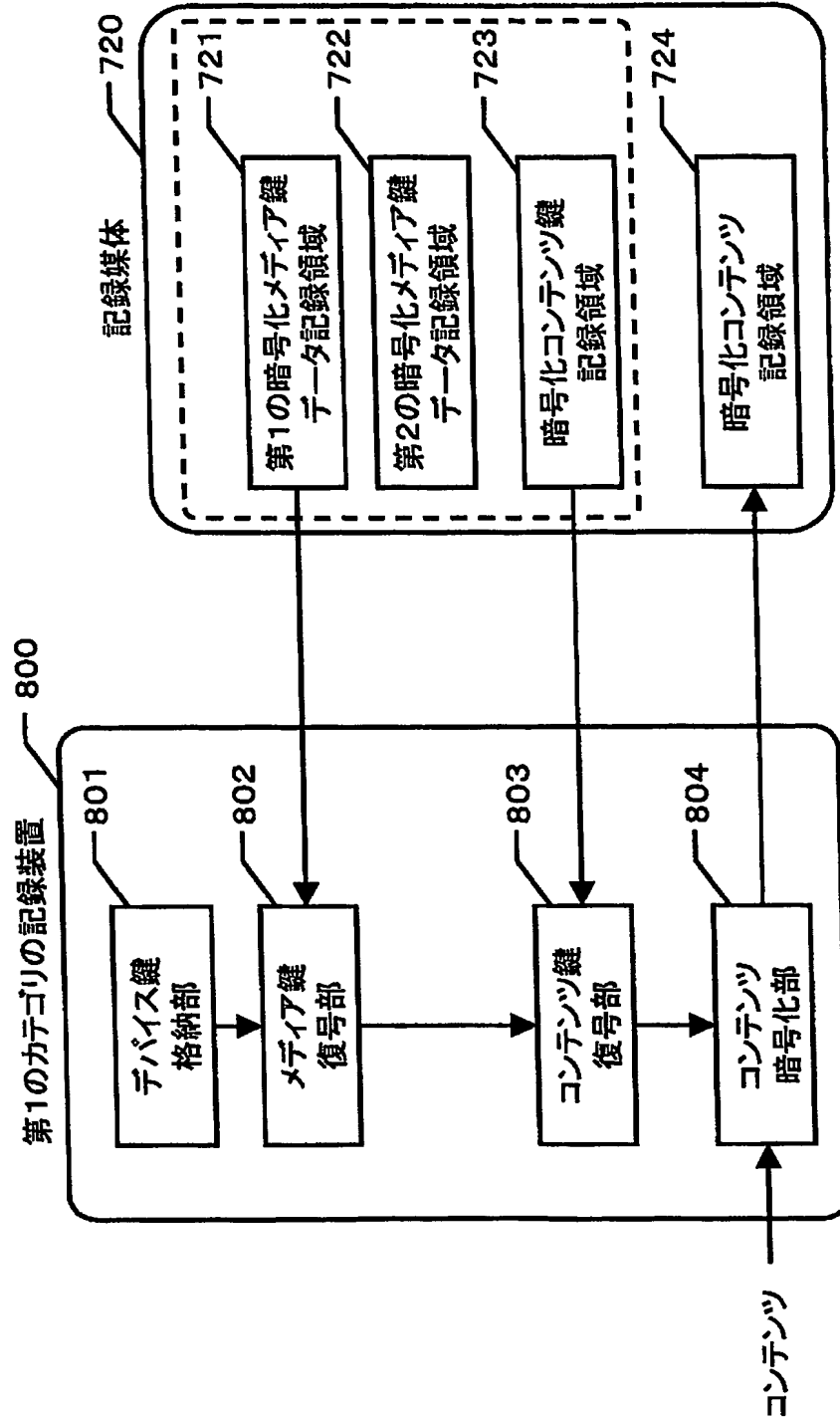
【図7】

本発明の実施の形態2における鍵生成装置及び記録媒体



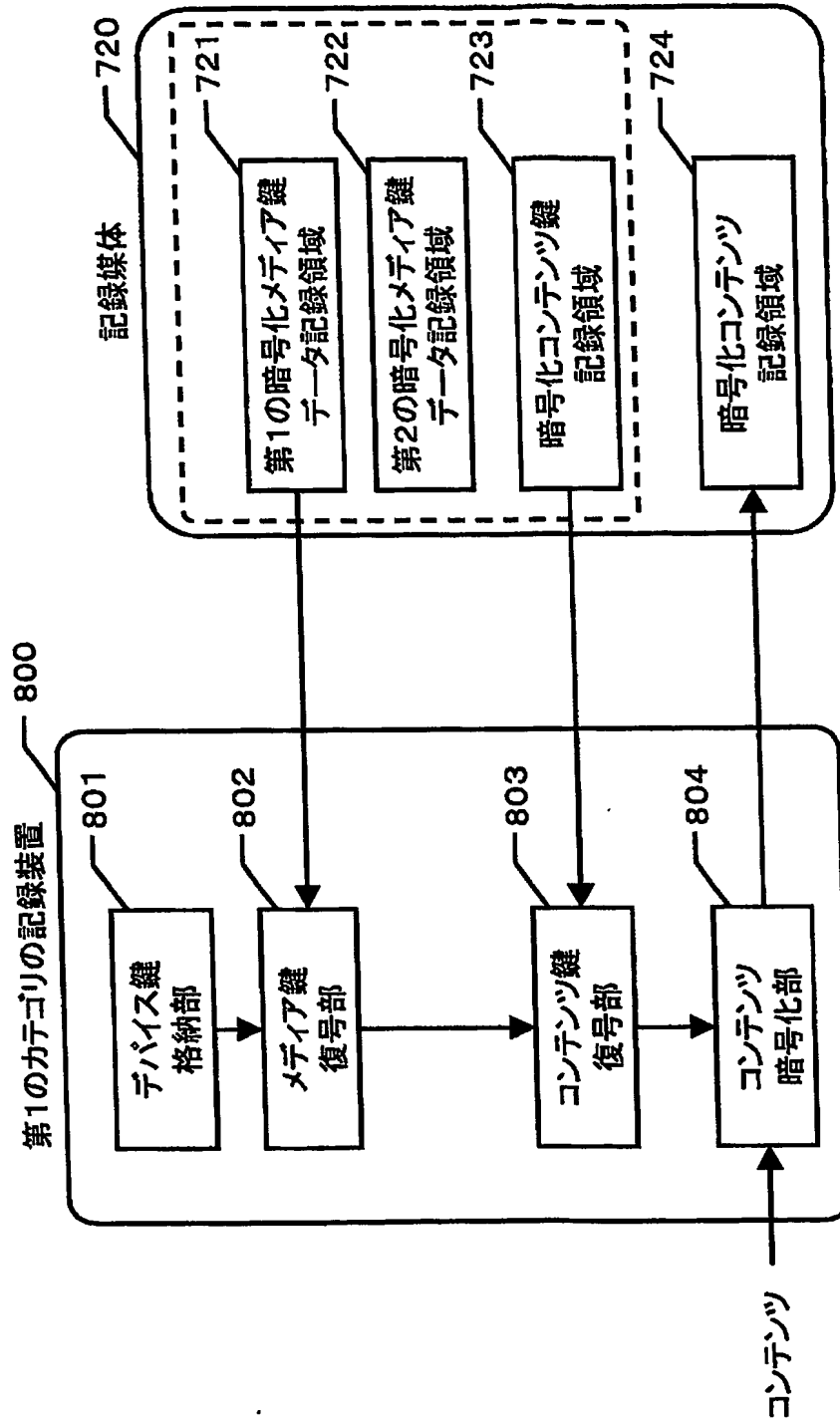
【図8】

本発明の実施の形態2における第1のカテゴリの記録装置及び記録媒体



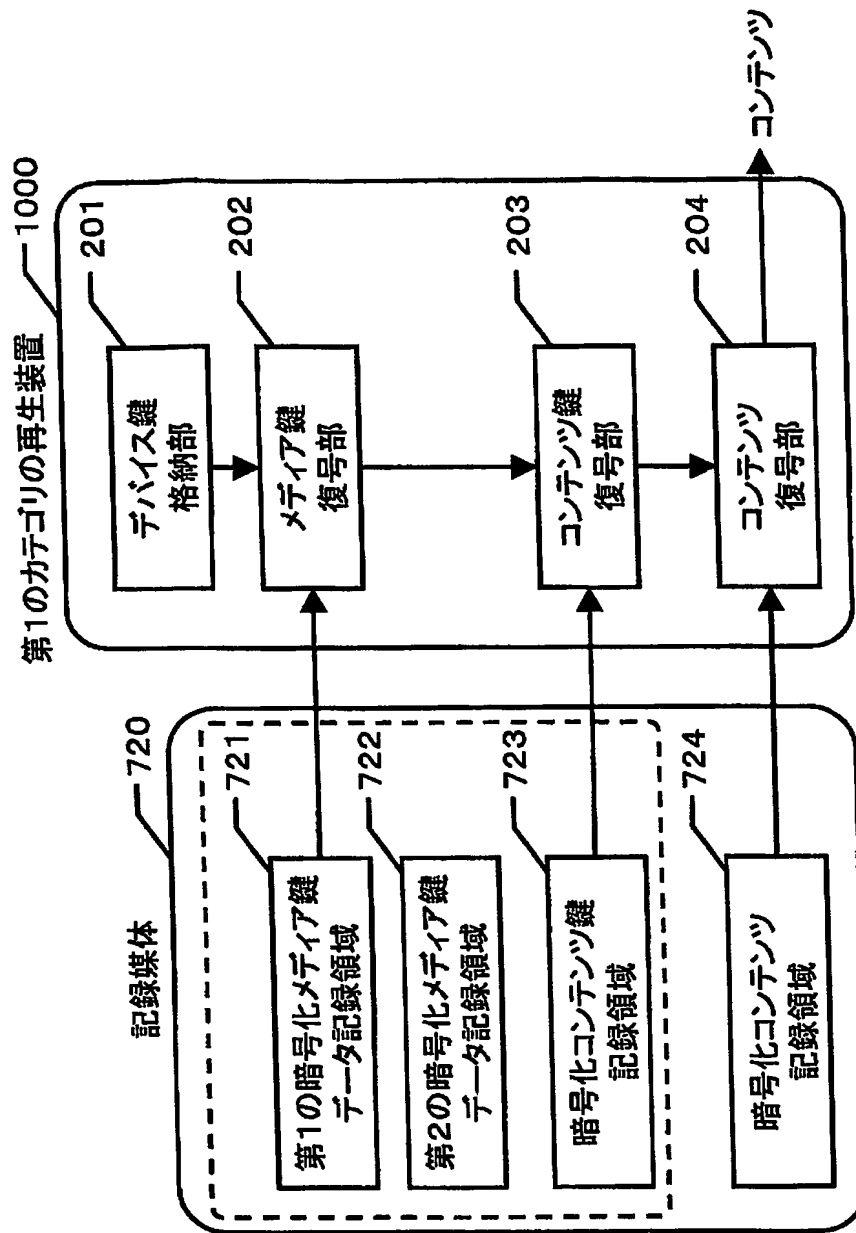
【図 9】

本発明の実施の形態2における第1のカテゴリの記録装置及び記録媒体



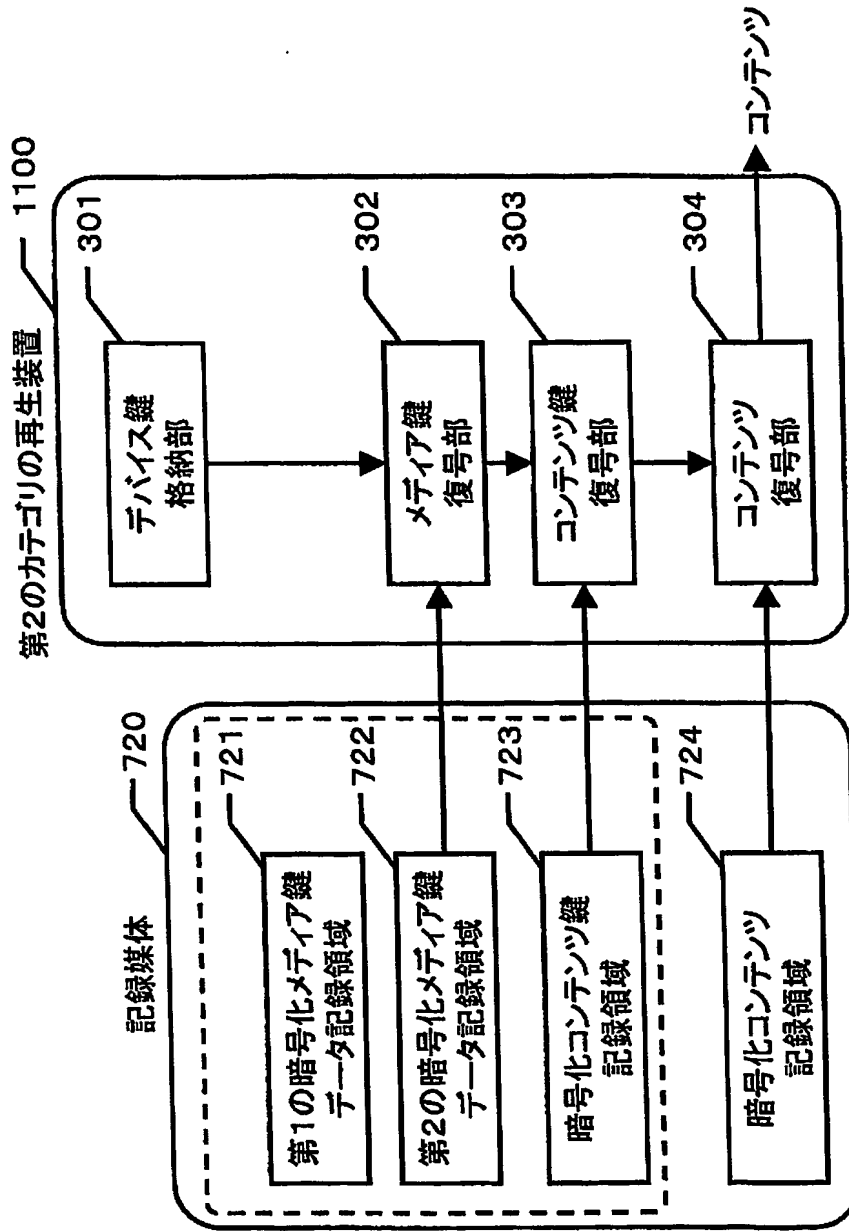
【図10】

本発明の実施の形態2における記録媒体及び第1のカテゴリの再生装置



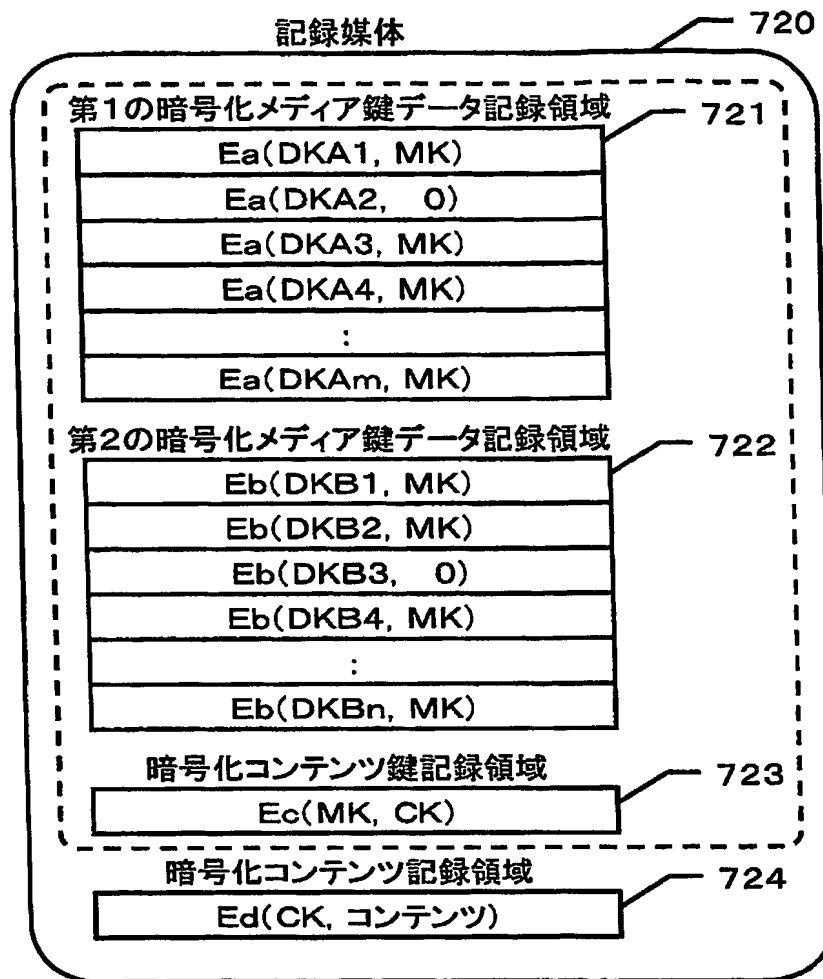
【図11】

本発明の実施の形態2における記録媒体及び第2のカテゴリの再生装置



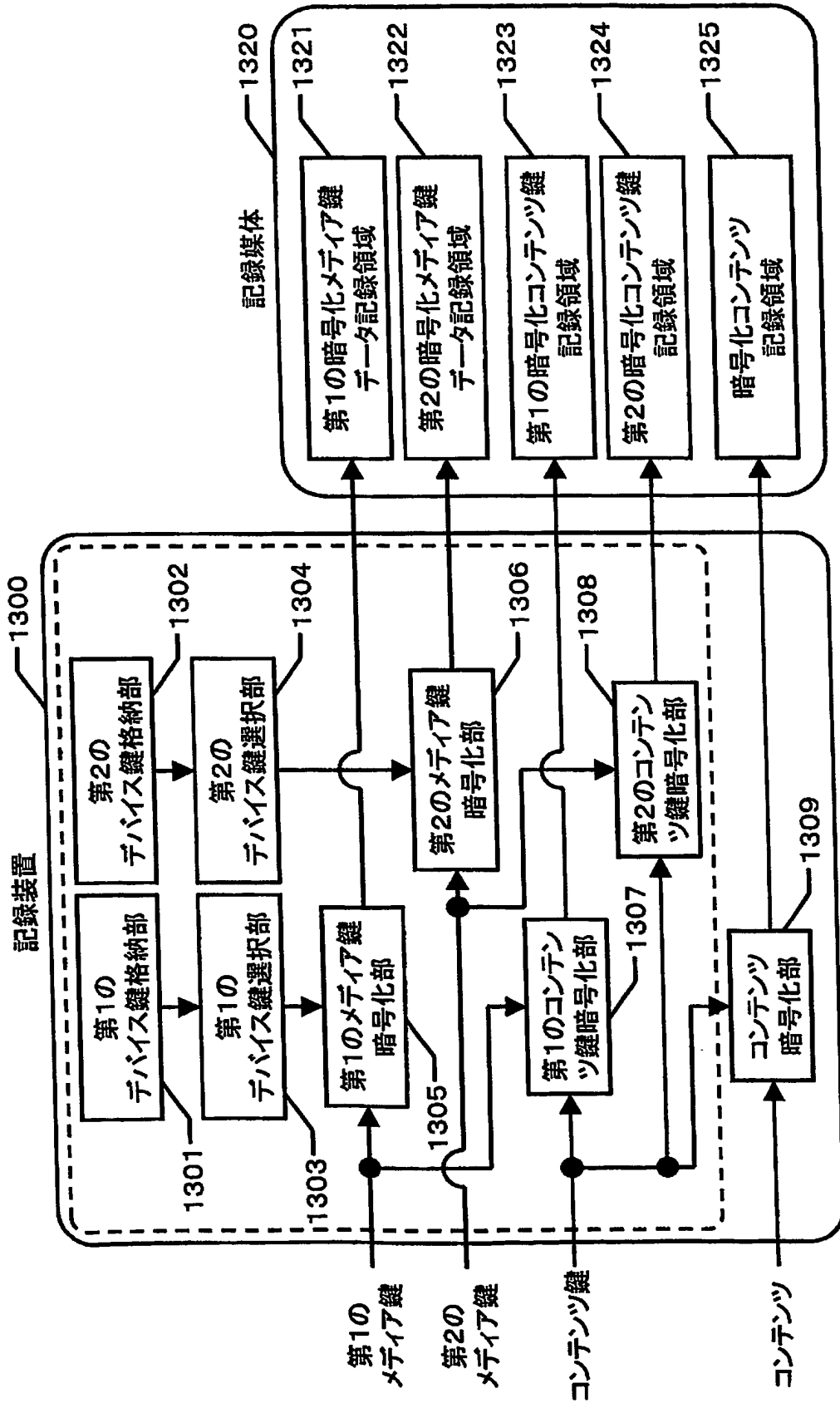
【図 12】

本発明の実施の形態2における記録媒体に記録するデータの具体例



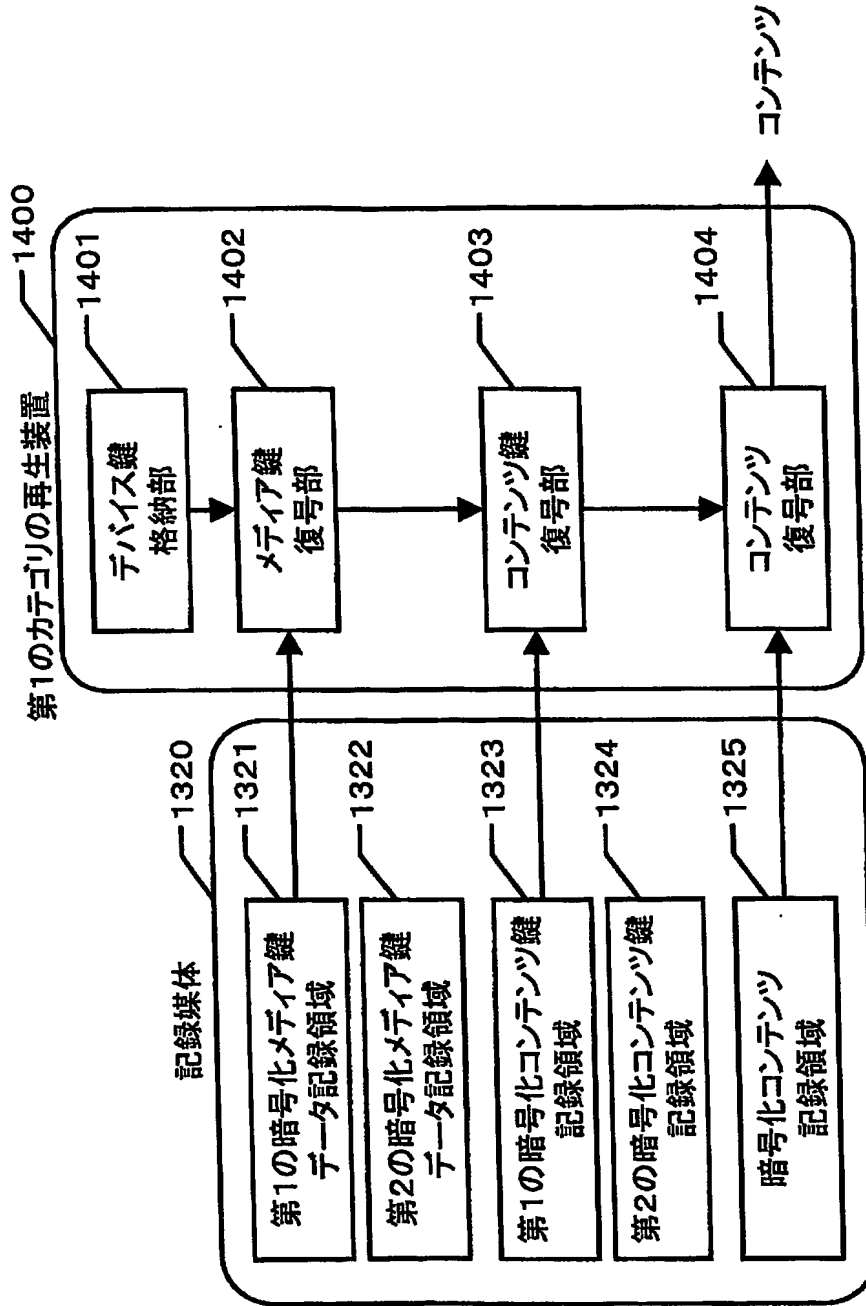
【図 13】

本発明の実施の形態3における記録装置及び記録媒体



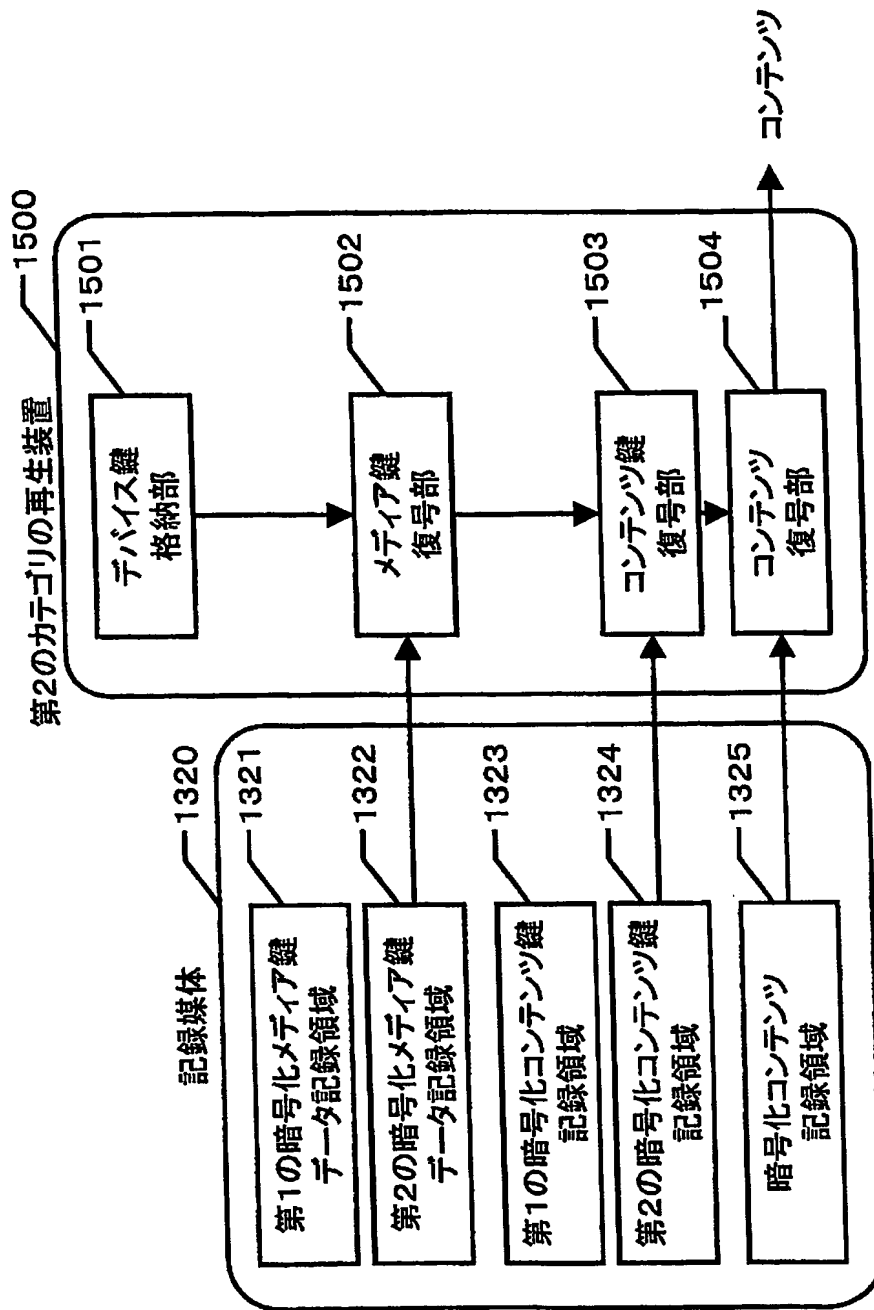
【図 14】

本発明の実施の形態3における記録媒体及び第1のカテゴリの再生装置



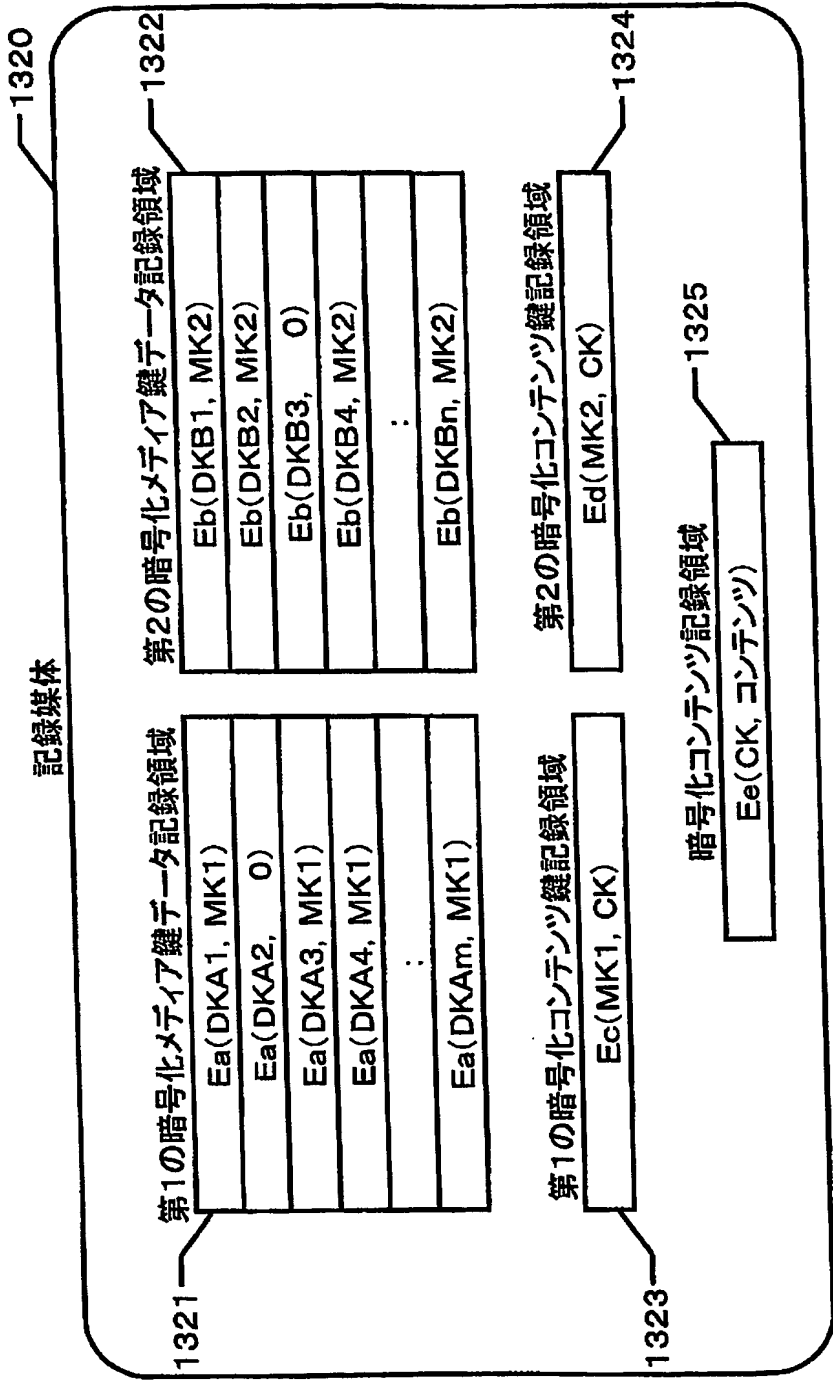
【図 15】

本発明の実施の形態3における記録媒体及び第2の再生装置



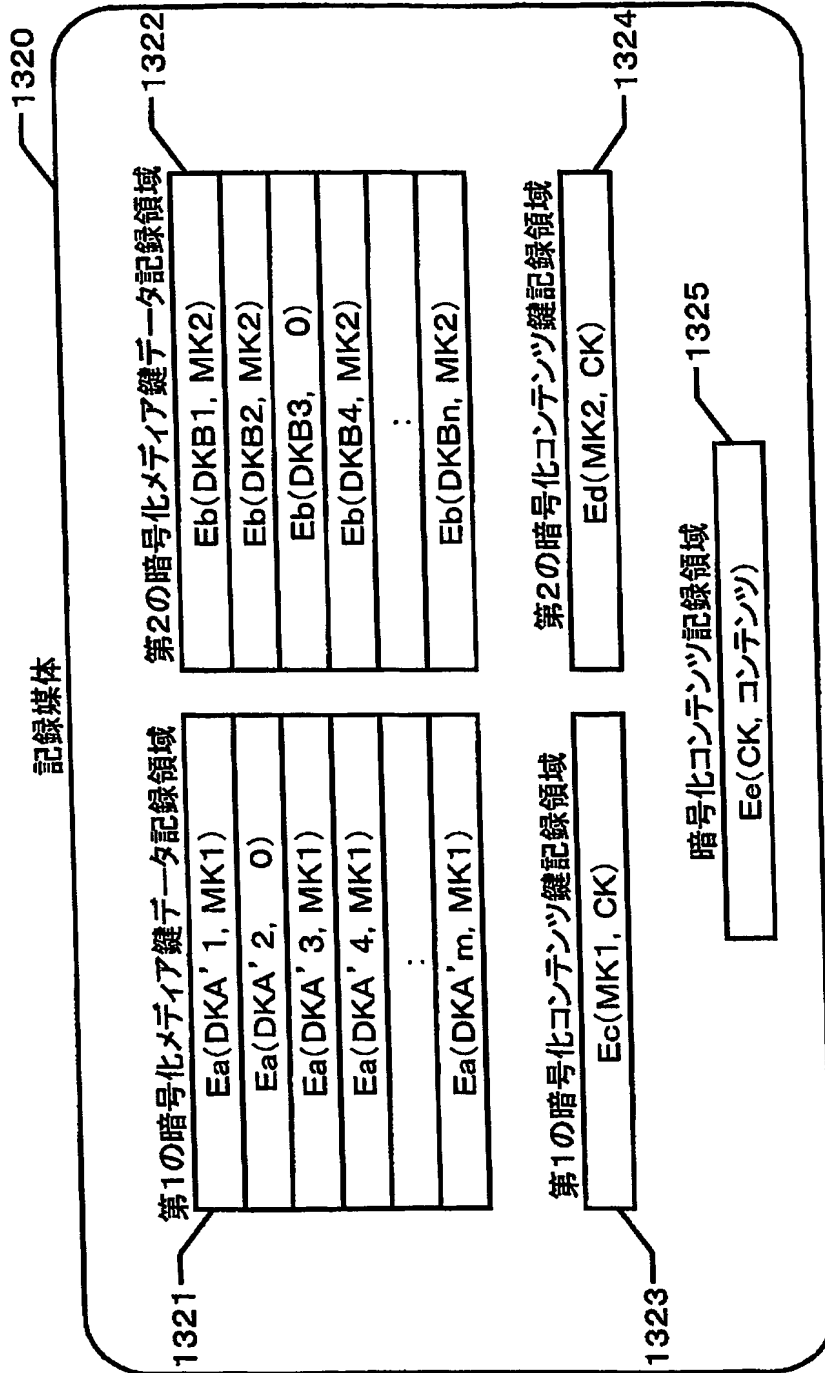
【図16】

本発明の実施の形態3における記録媒体に記録するデータの具体例



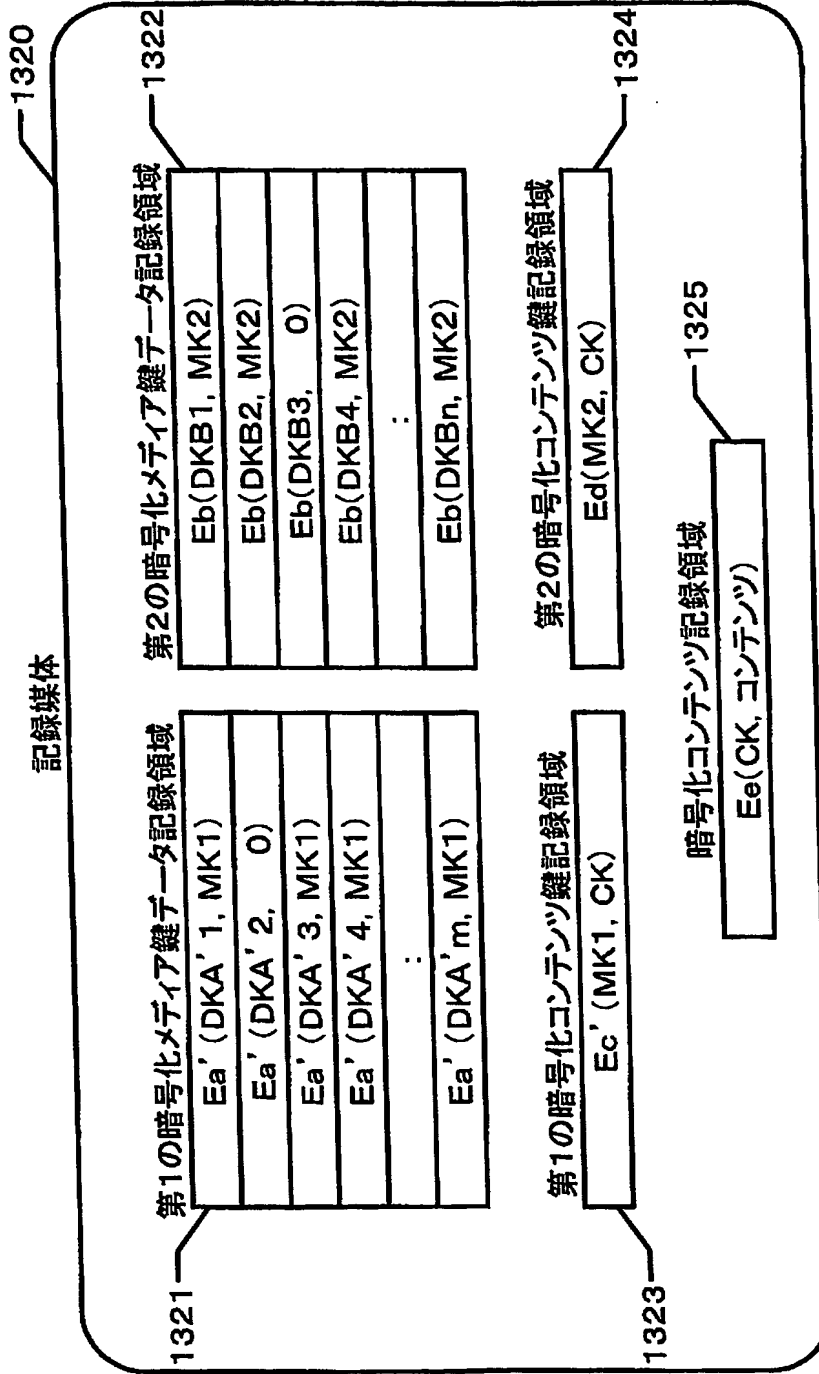
【図 17】

本発明の実施の形態3におけるシステム更新の具体例1



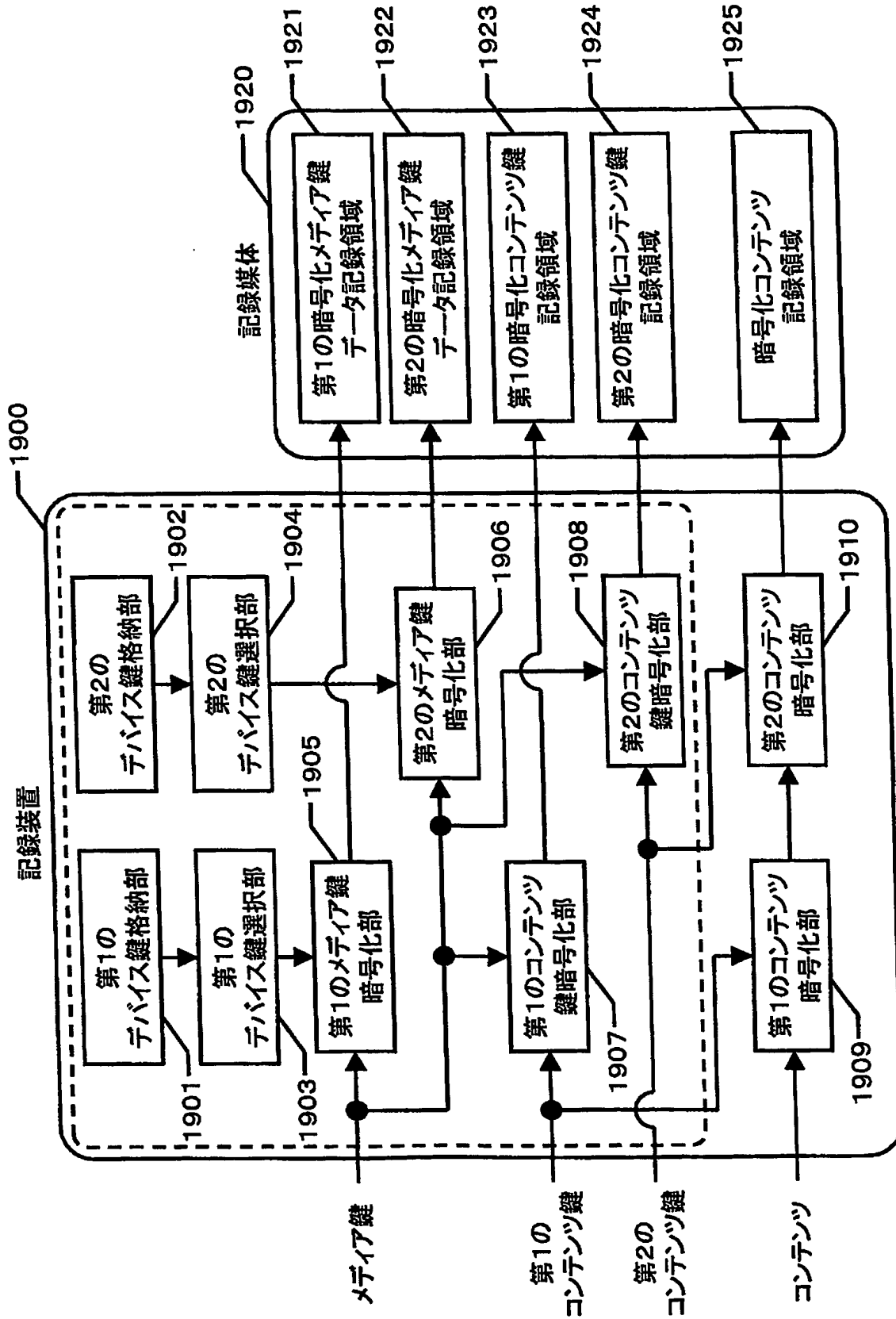
【図18】

本発明の実施の形態3におけるシステム更新の具体例2



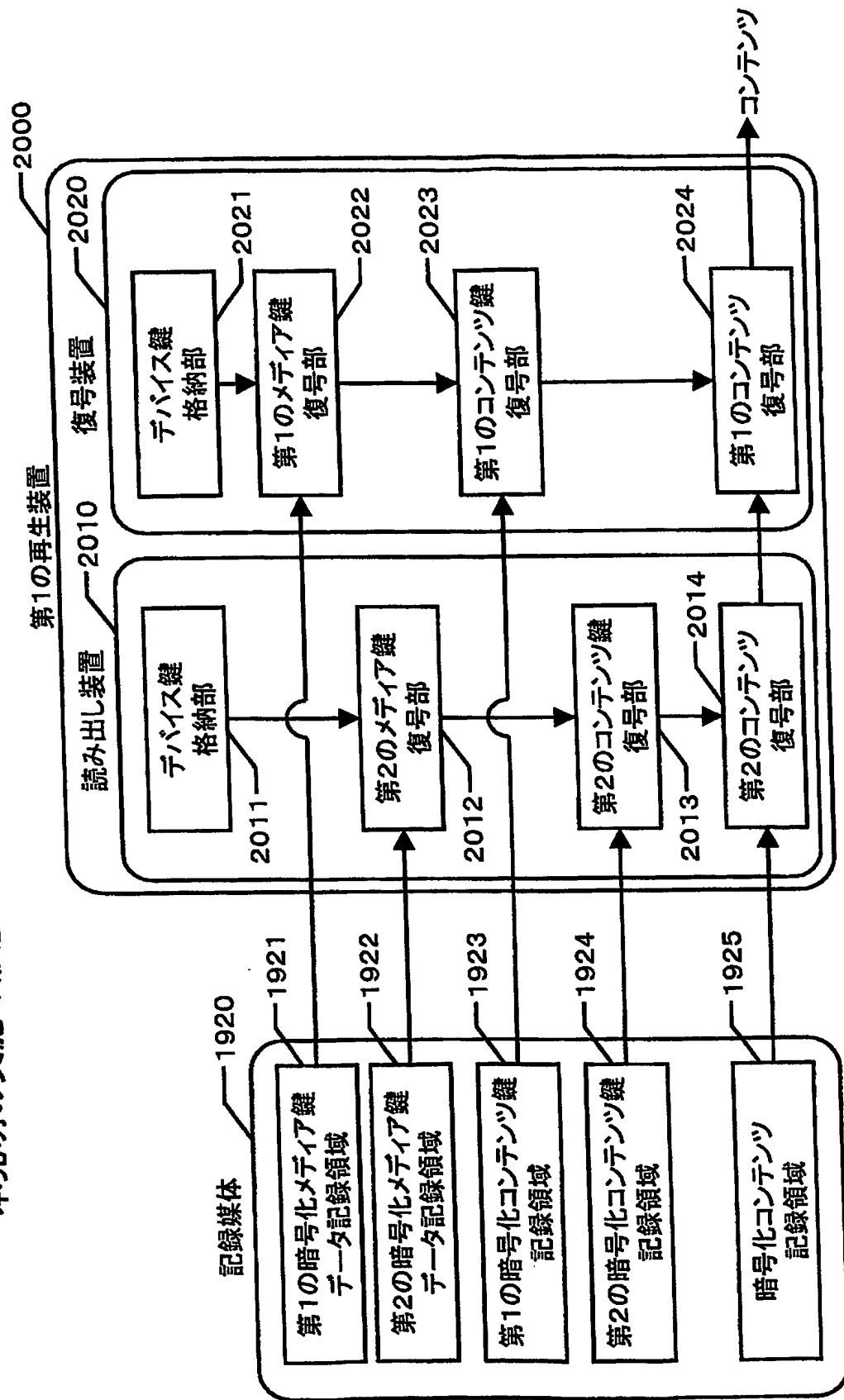
【図19】

本発明の実施の形態4における記録装置及び記録媒体



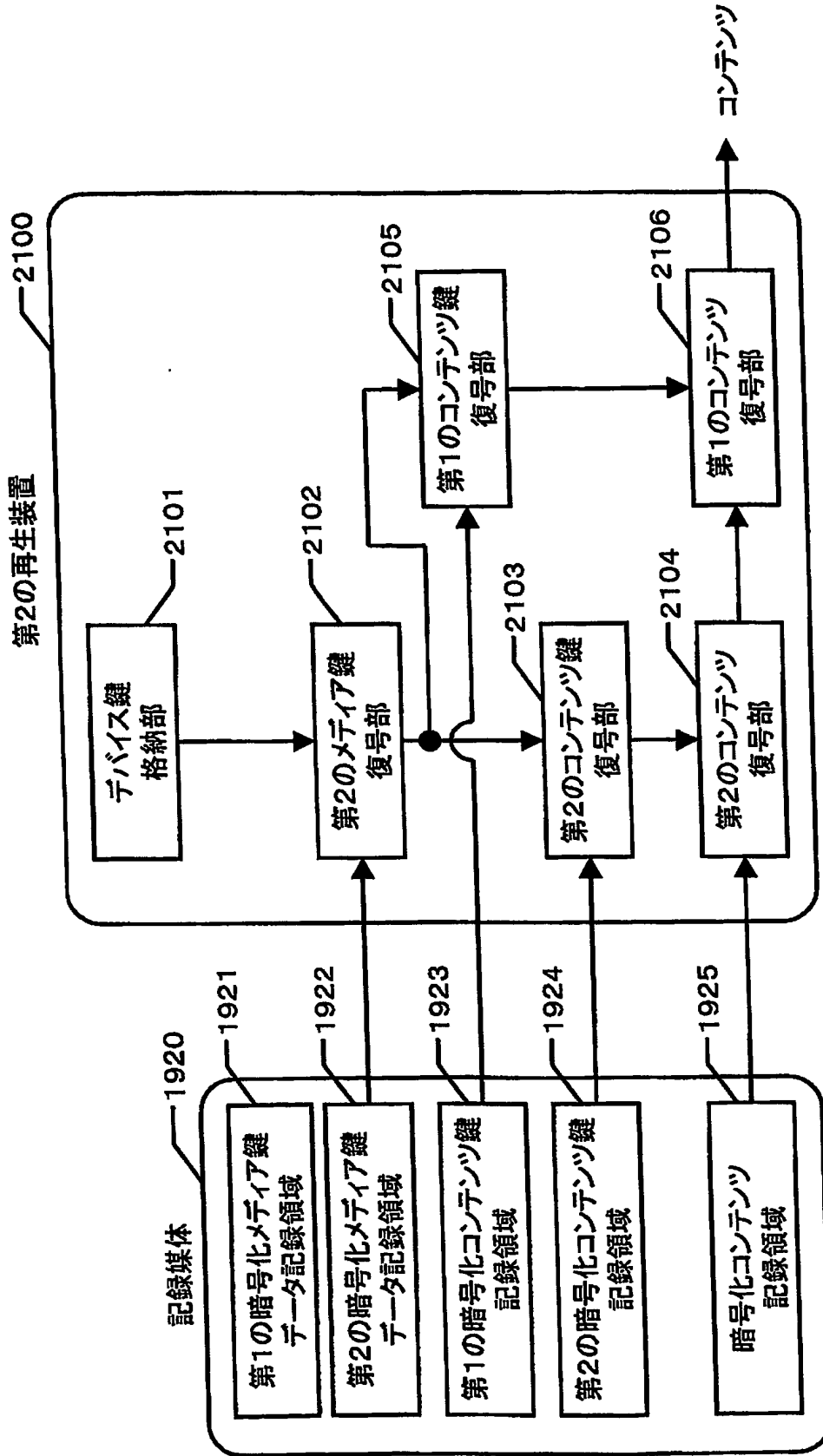
【図20】

本発明の実施の形態4における記録媒体及び第1の再生装置



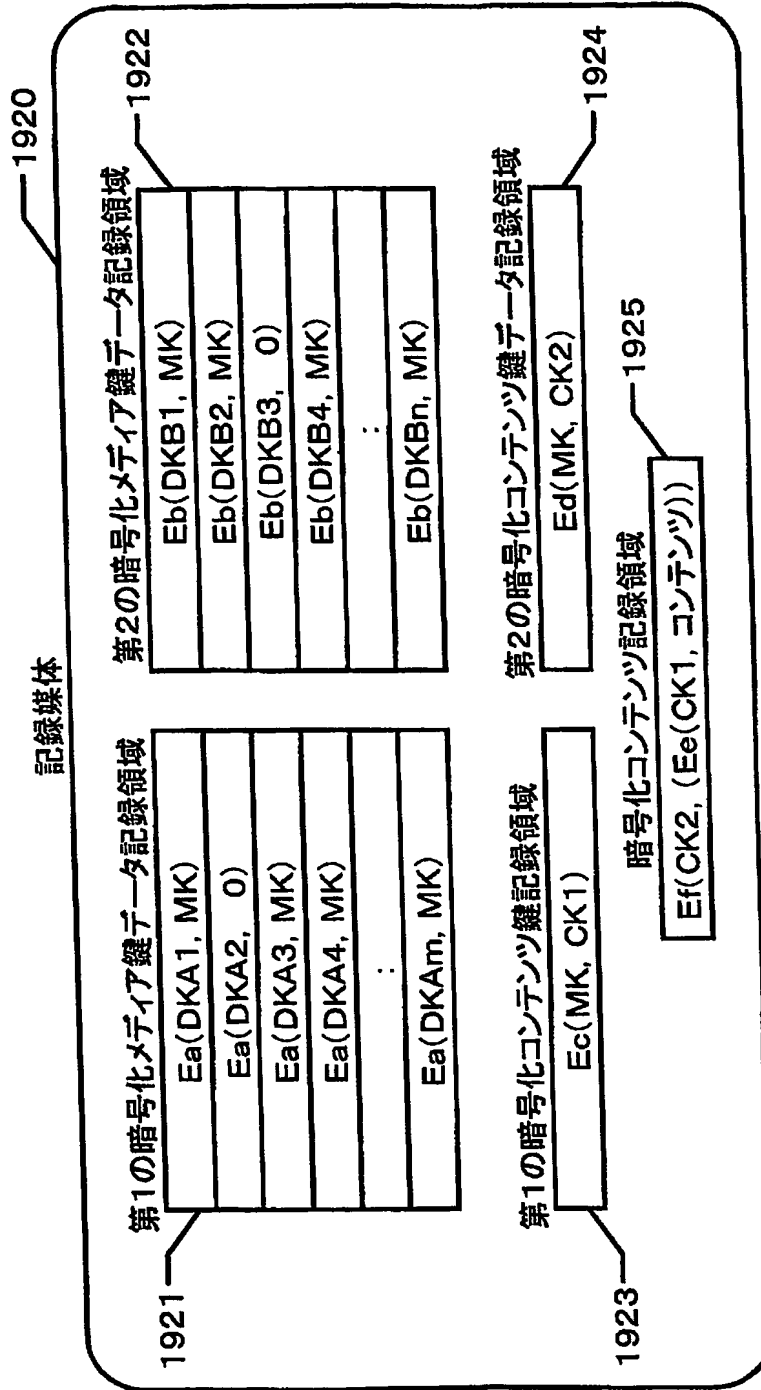
【図21】

本発明の実施の形態4における記録媒体及び第2の再生装置



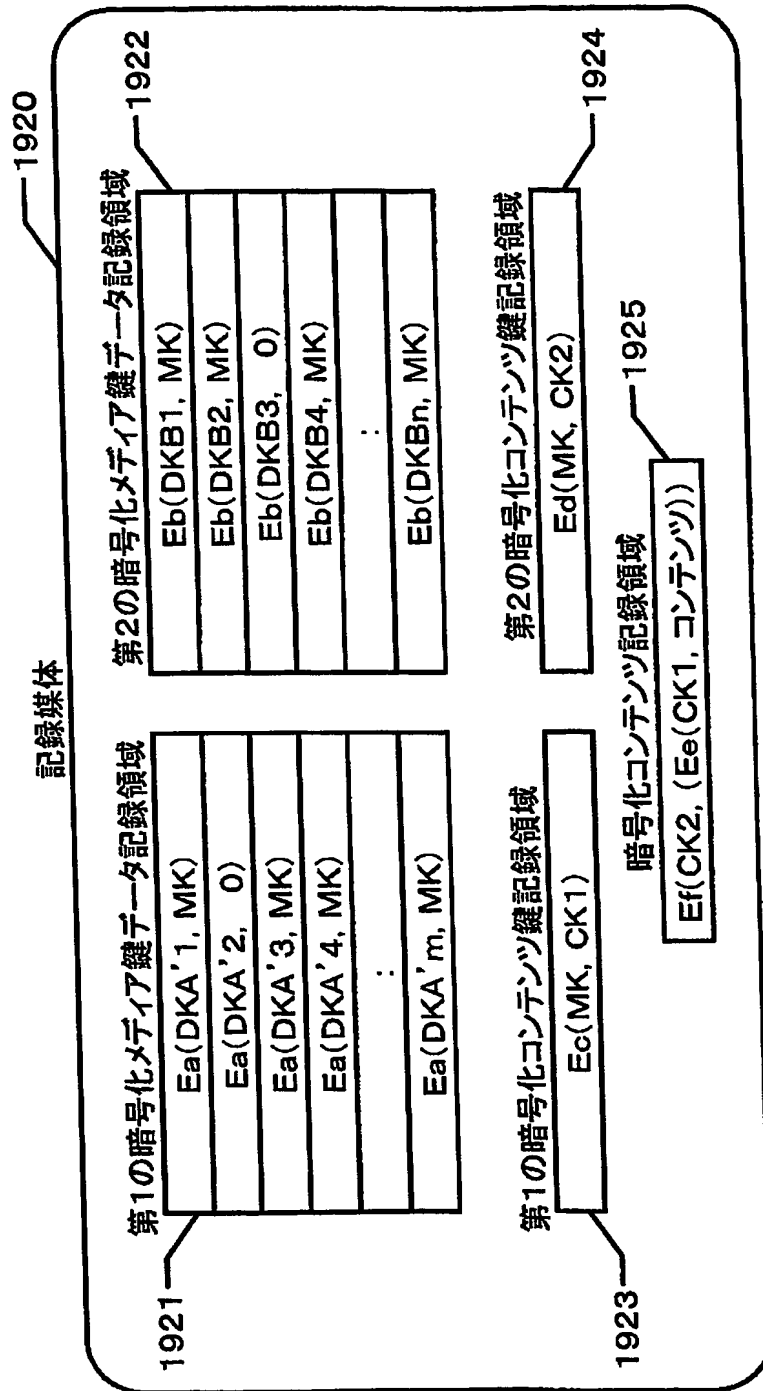
【図 22】

本発明の実施の形態4における記録媒体に記録するデータの具体例



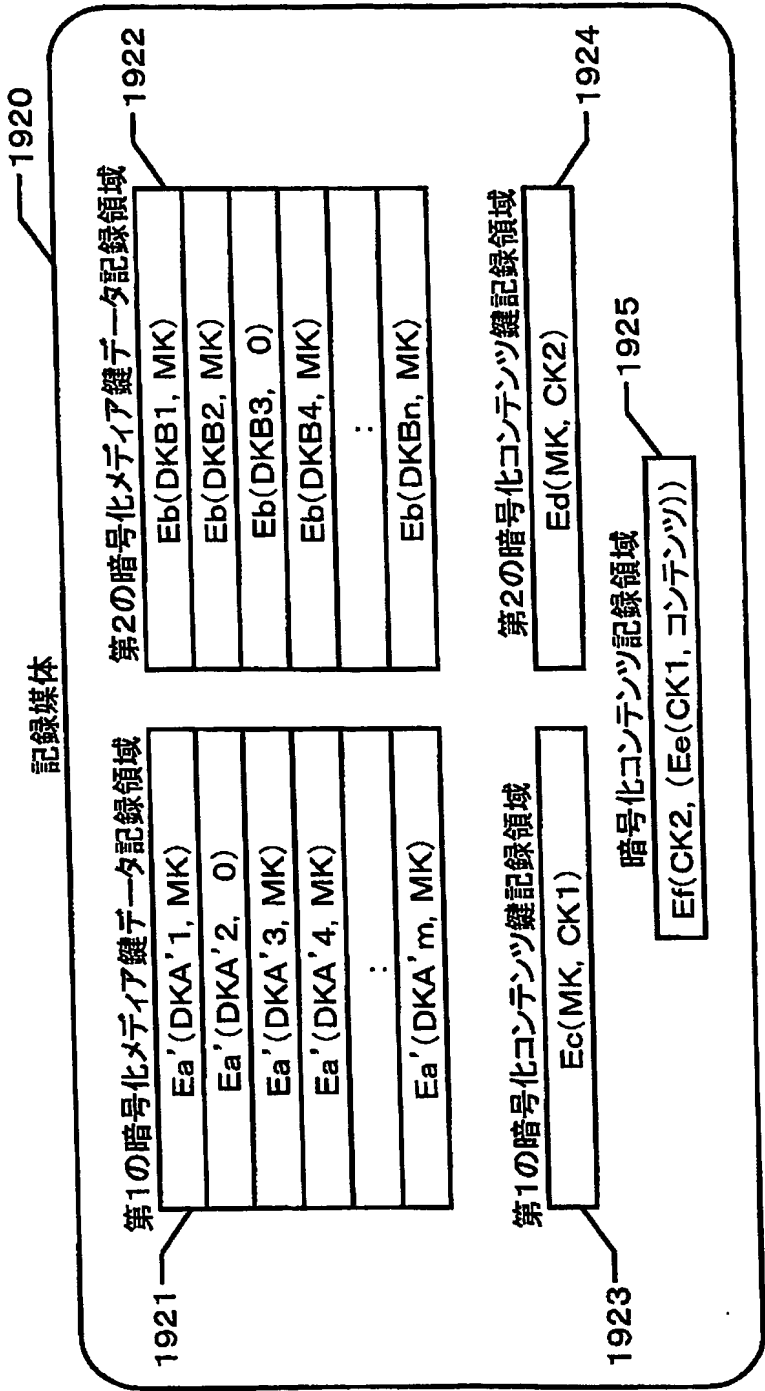
【図 23】

本発明の実施の形態4におけるシステム更新の具体例1



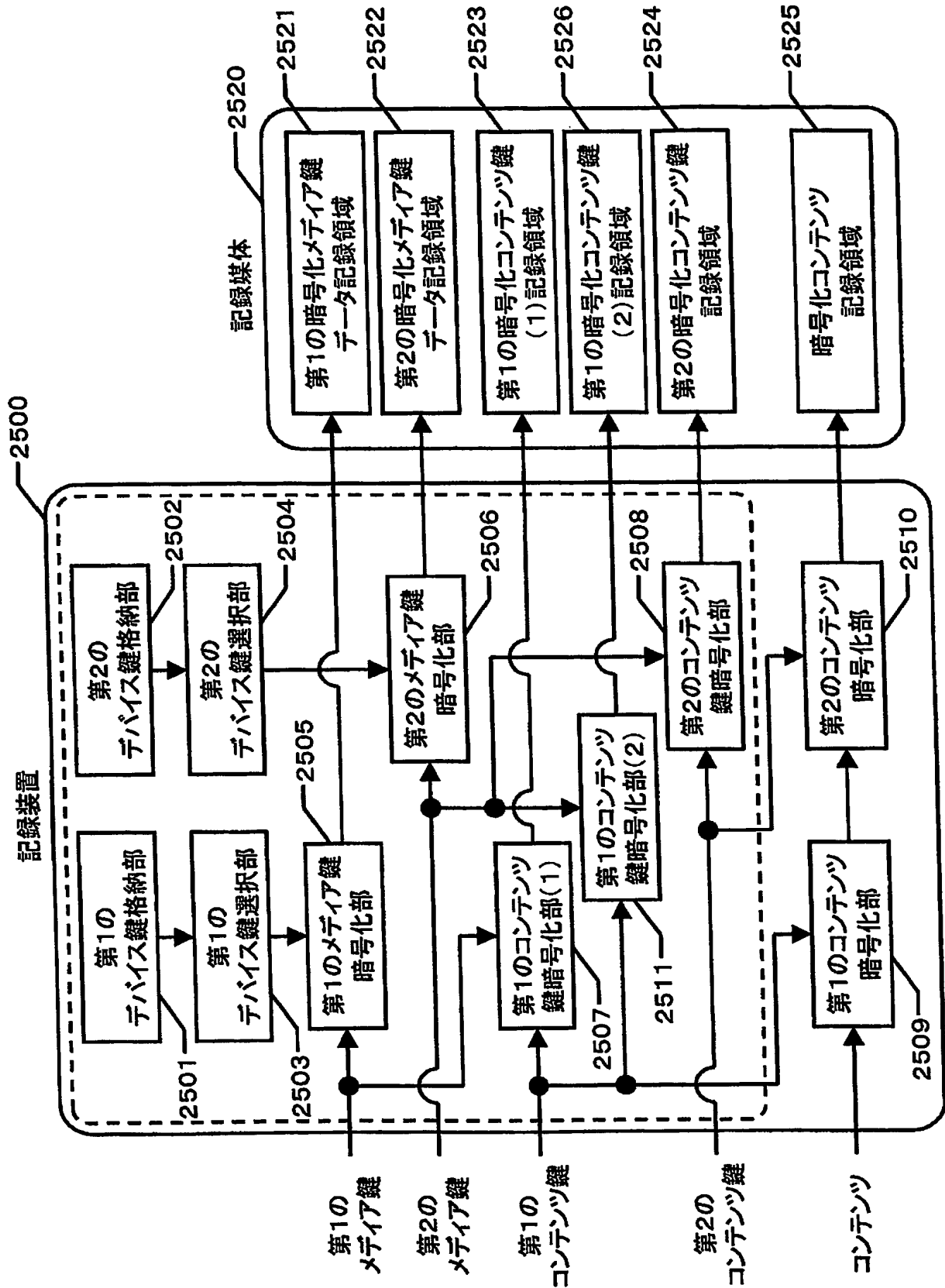
【図 2 4】

本発明の実施の形態 4 におけるシステム更新の具体例 2



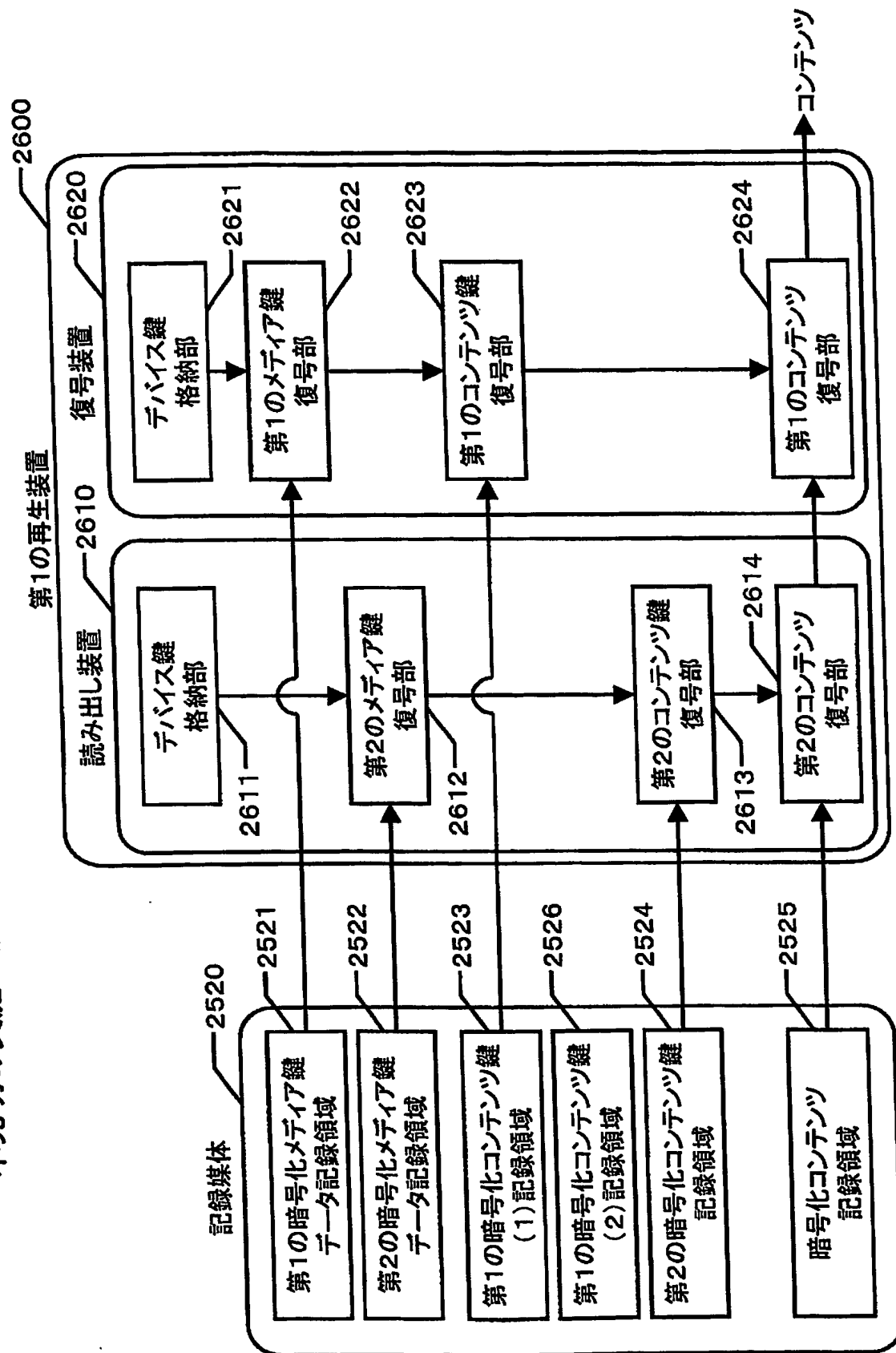
【図 25】

本発明の実施の形態5における記録装置及び記録媒体



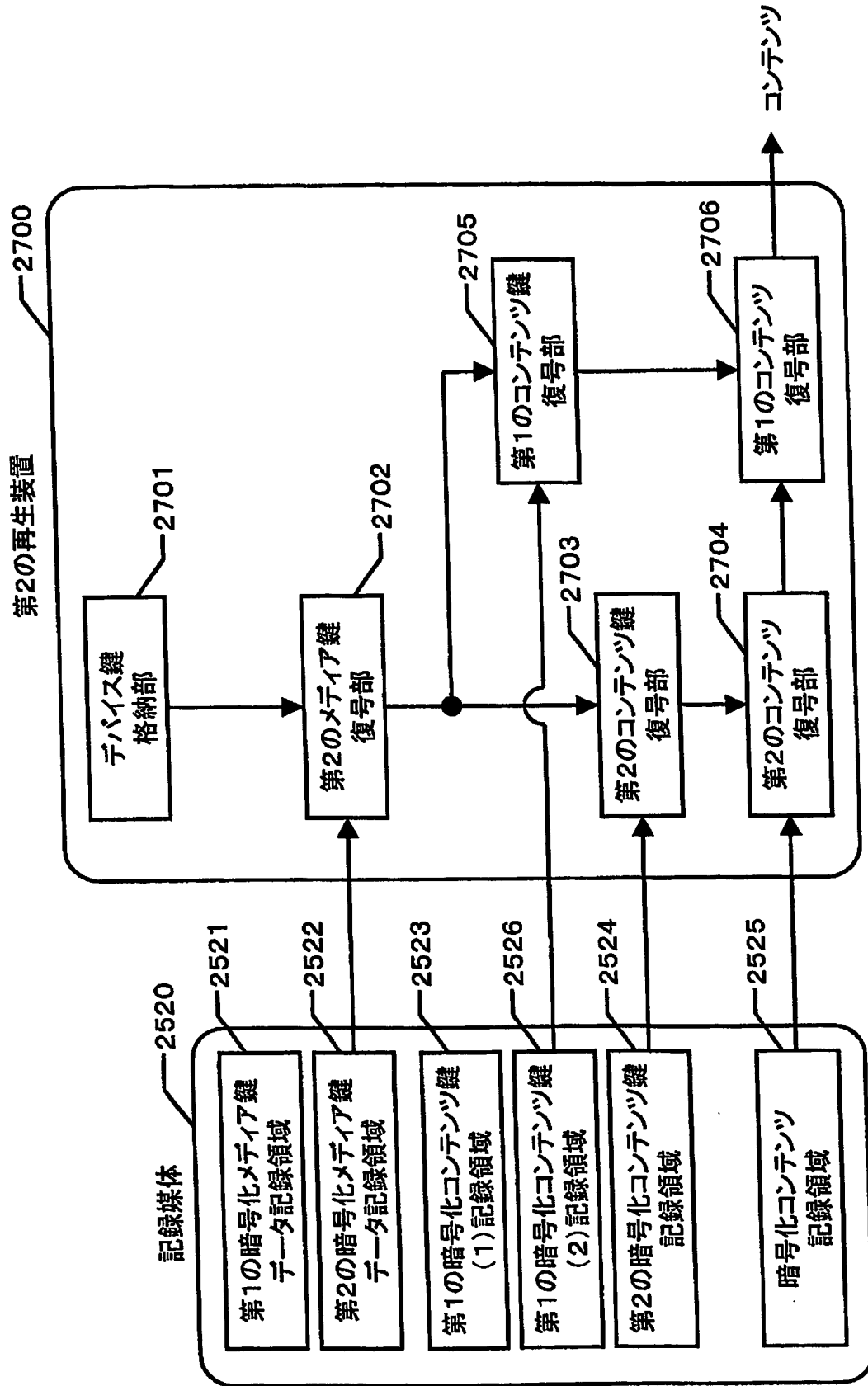
【図 26】

本発明の実施の形態5における記録媒体及び第1の再生装置



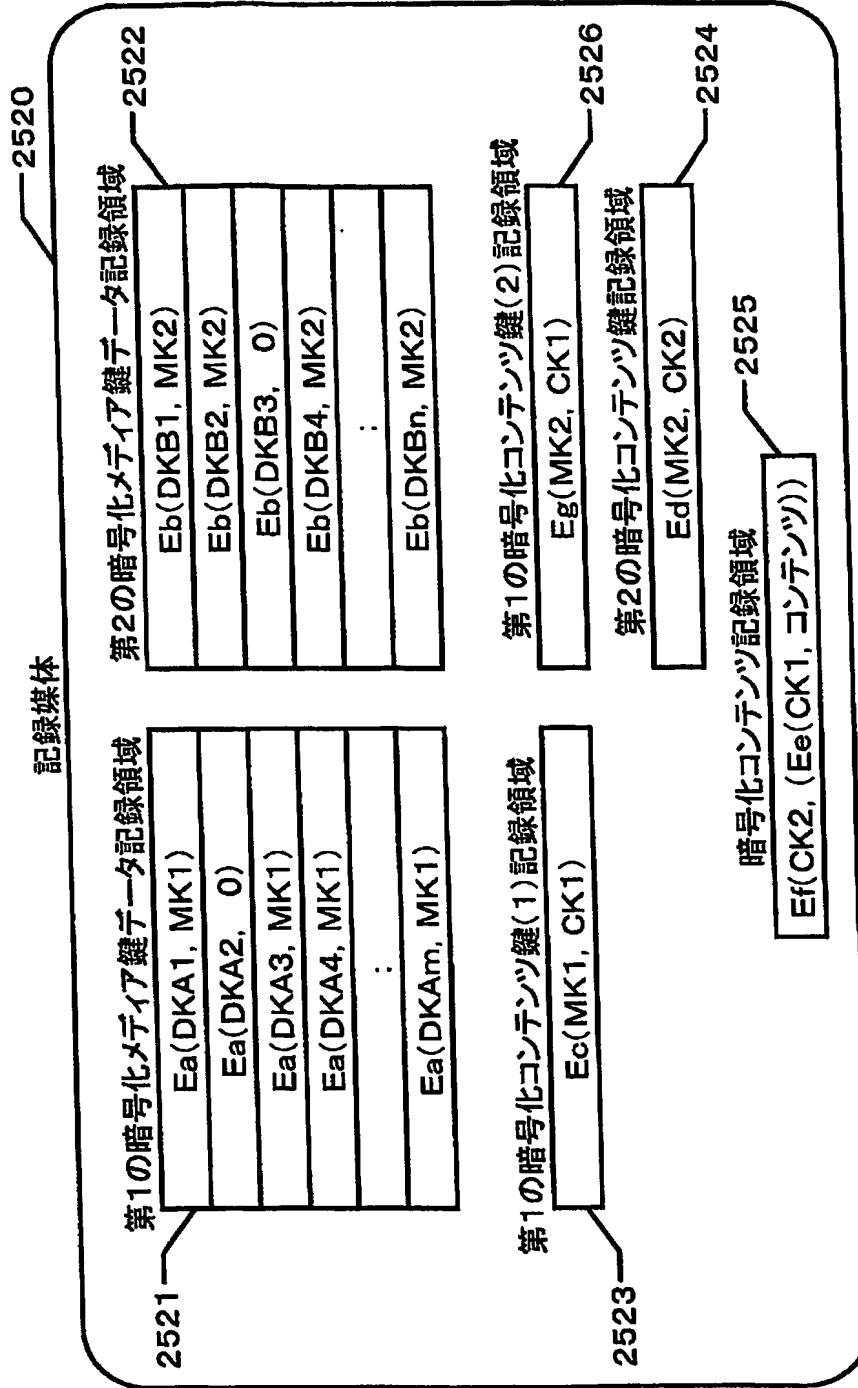
【図27】

本発明の実施の形態5における記録媒体及び第2の再生装置



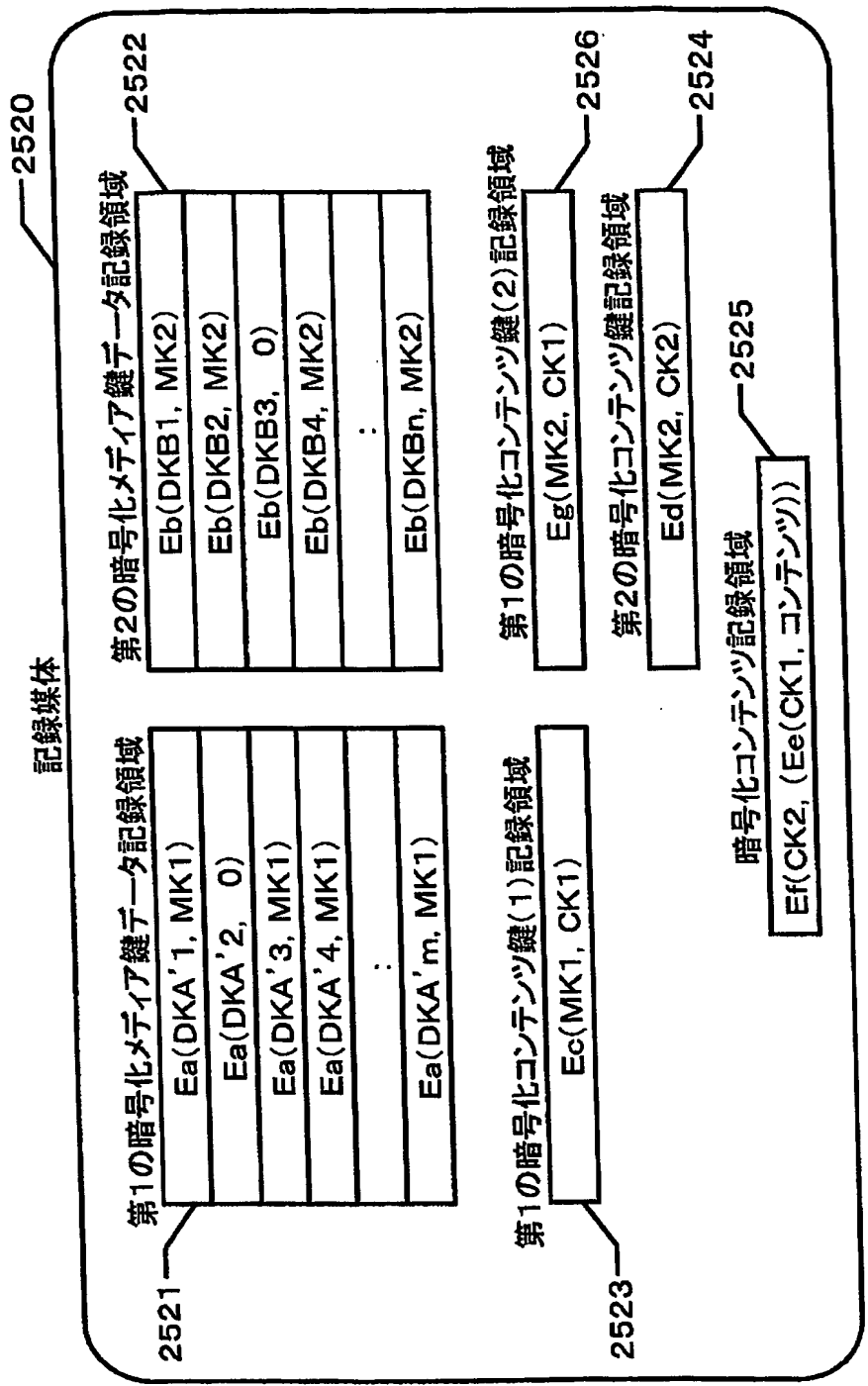
【図28】

本発明の実施の形態5における記録媒体に記録するデータの実体例



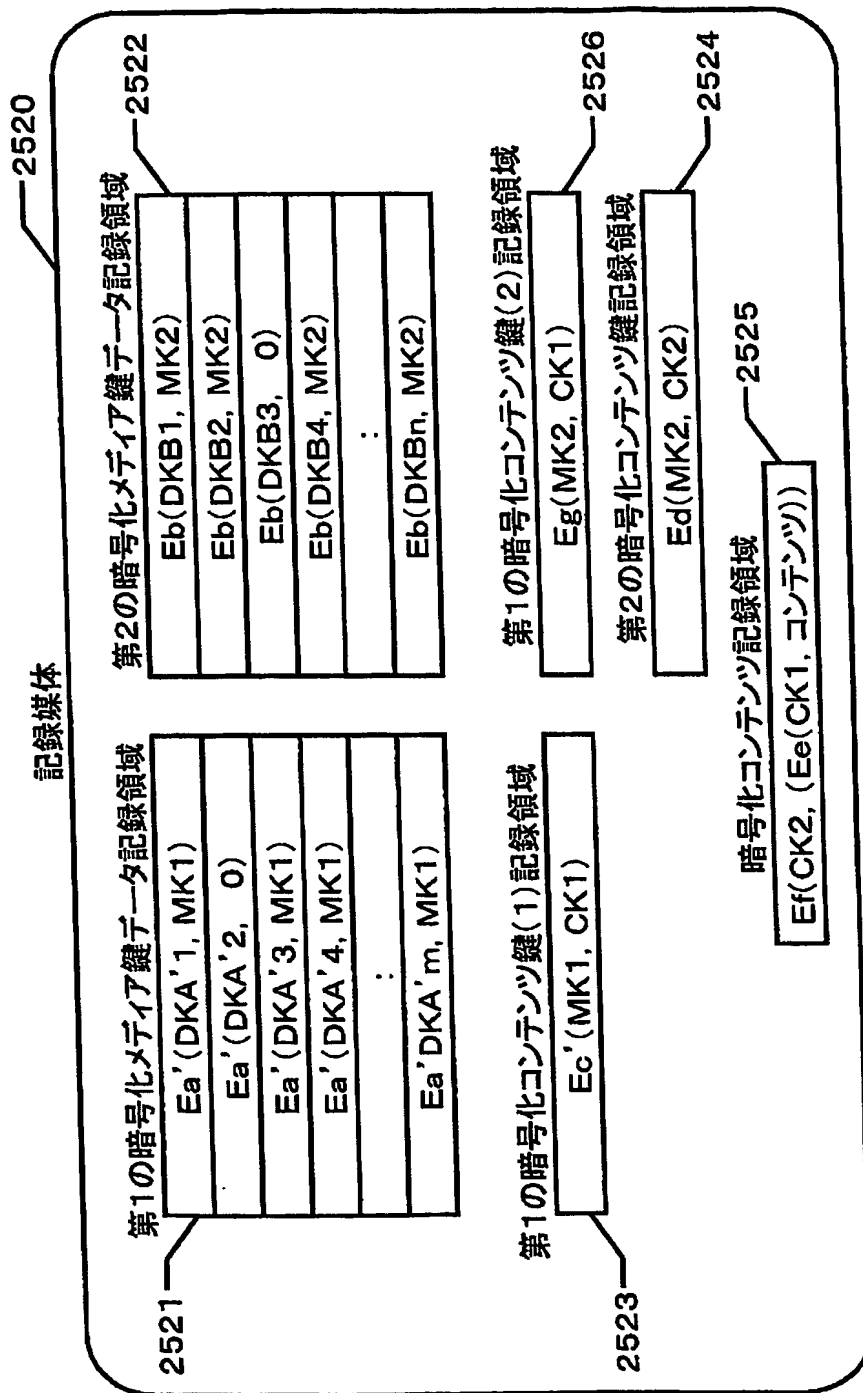
【図29】

本発明の実施の形態5におけるシステム更新の具体例1



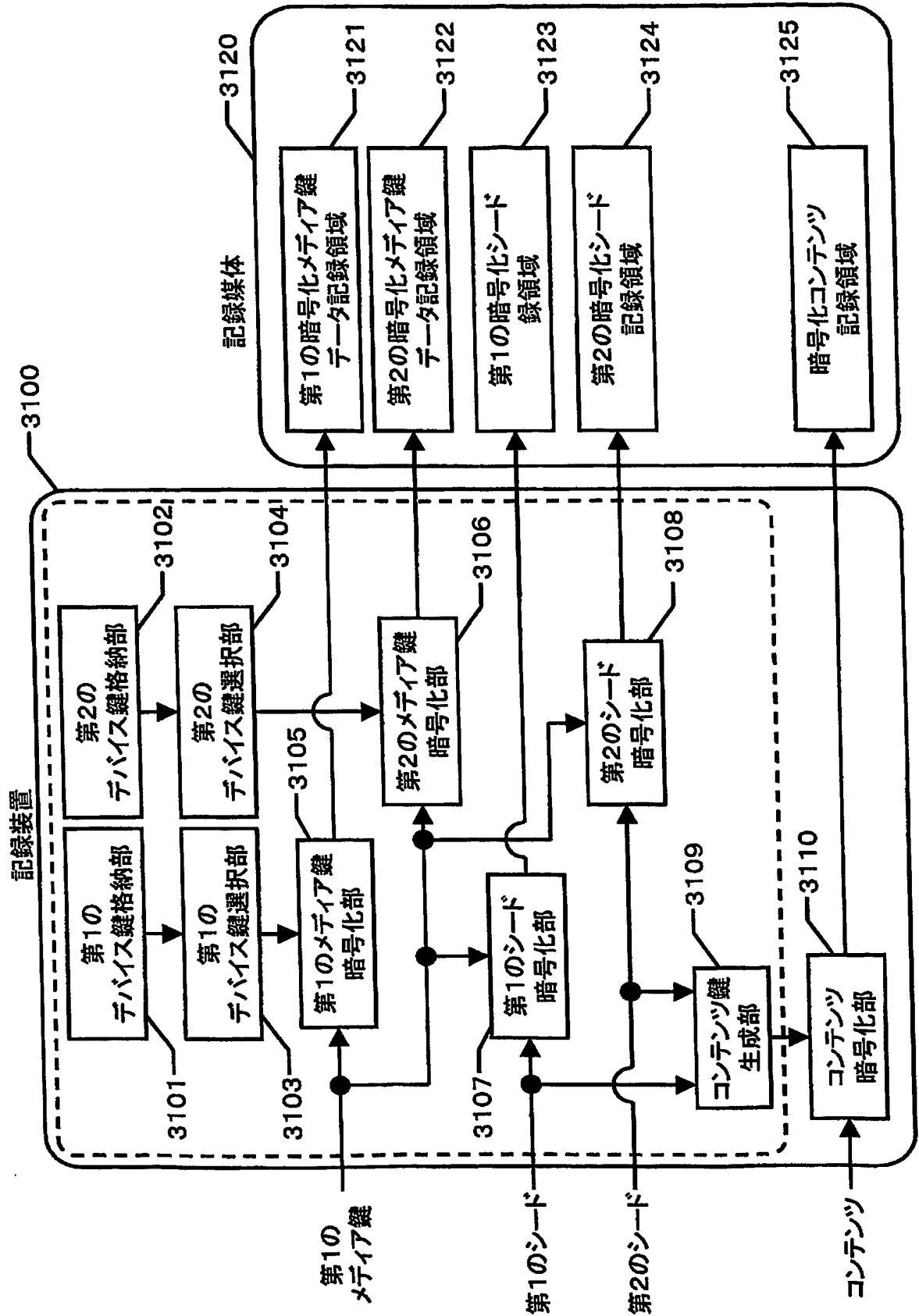
【図30】

本発明の実施の形態5におけるシステム更新の具体例2



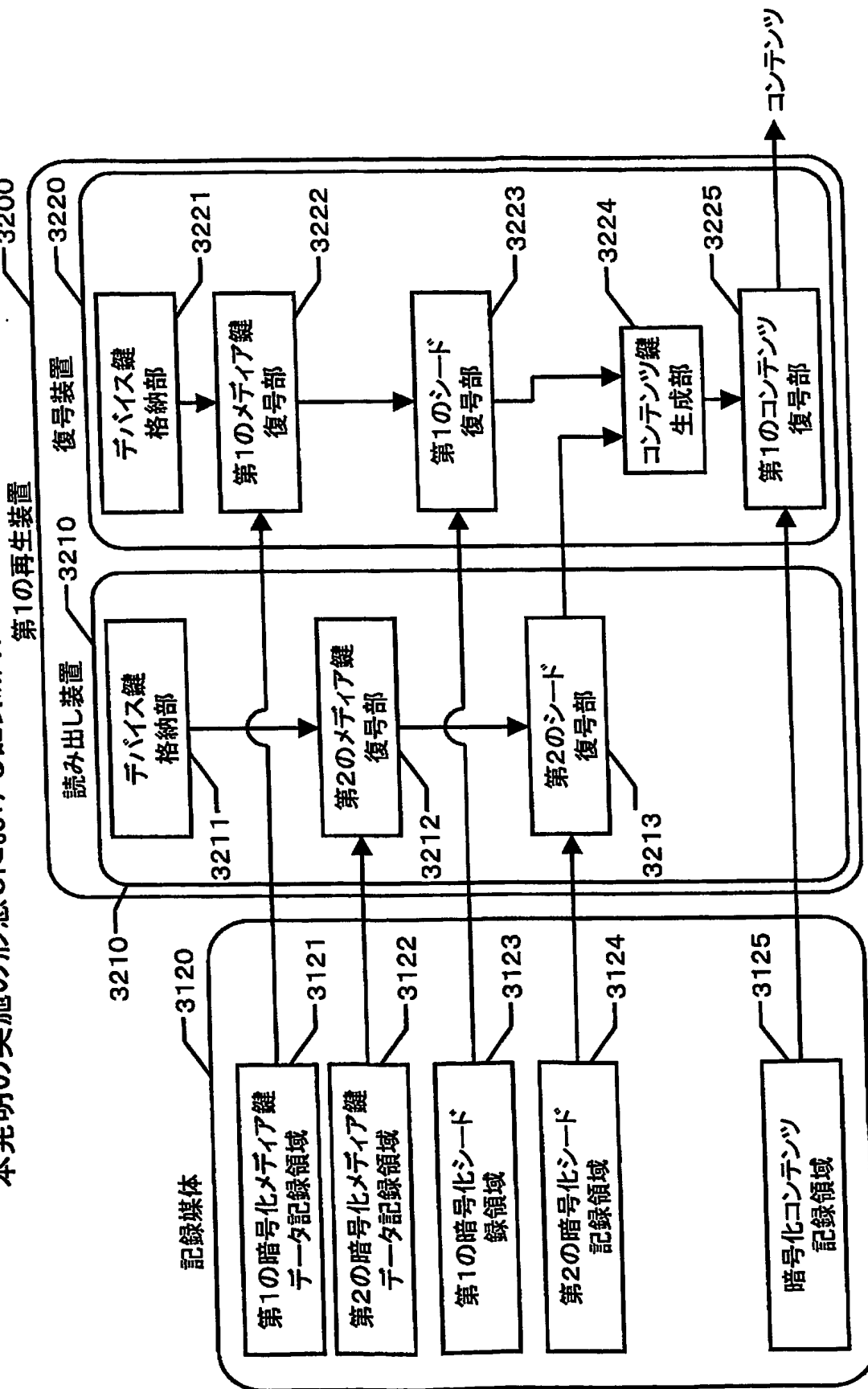
【図 31】

本発明の実施の形態6における記録装置及び記録媒体



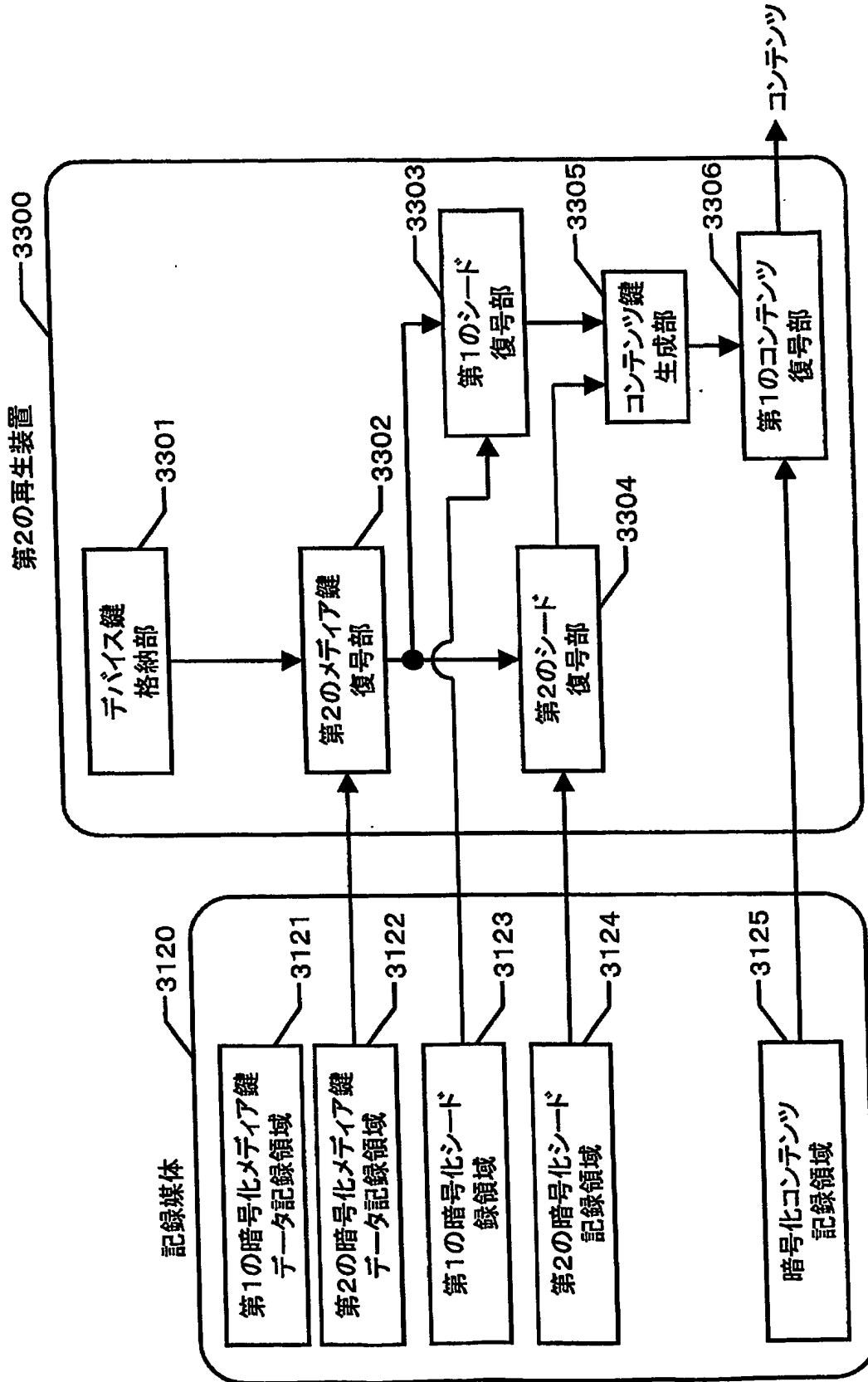
【図32】

本発明の実施の形態6における記録媒体及び第1の再生装置



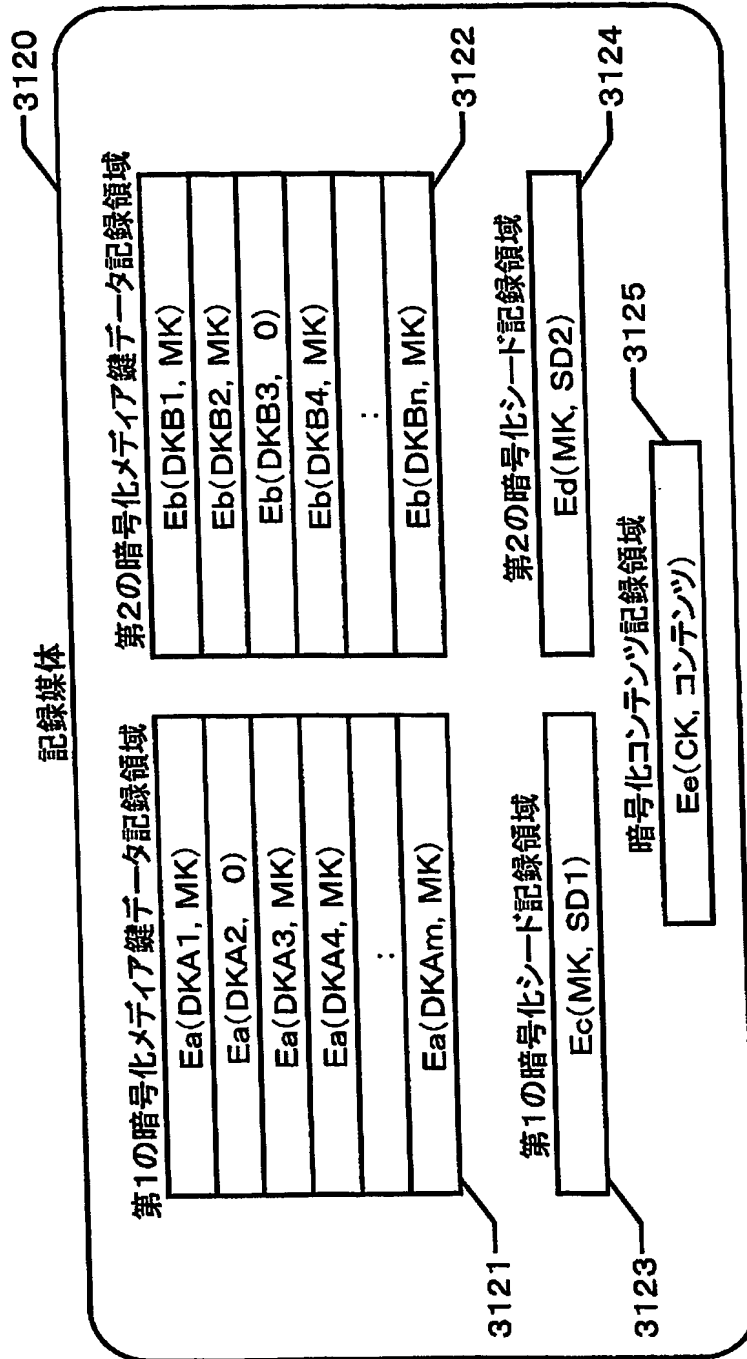
【図33】

本発明の実施の形態6における記録媒体及び第2の再生装置



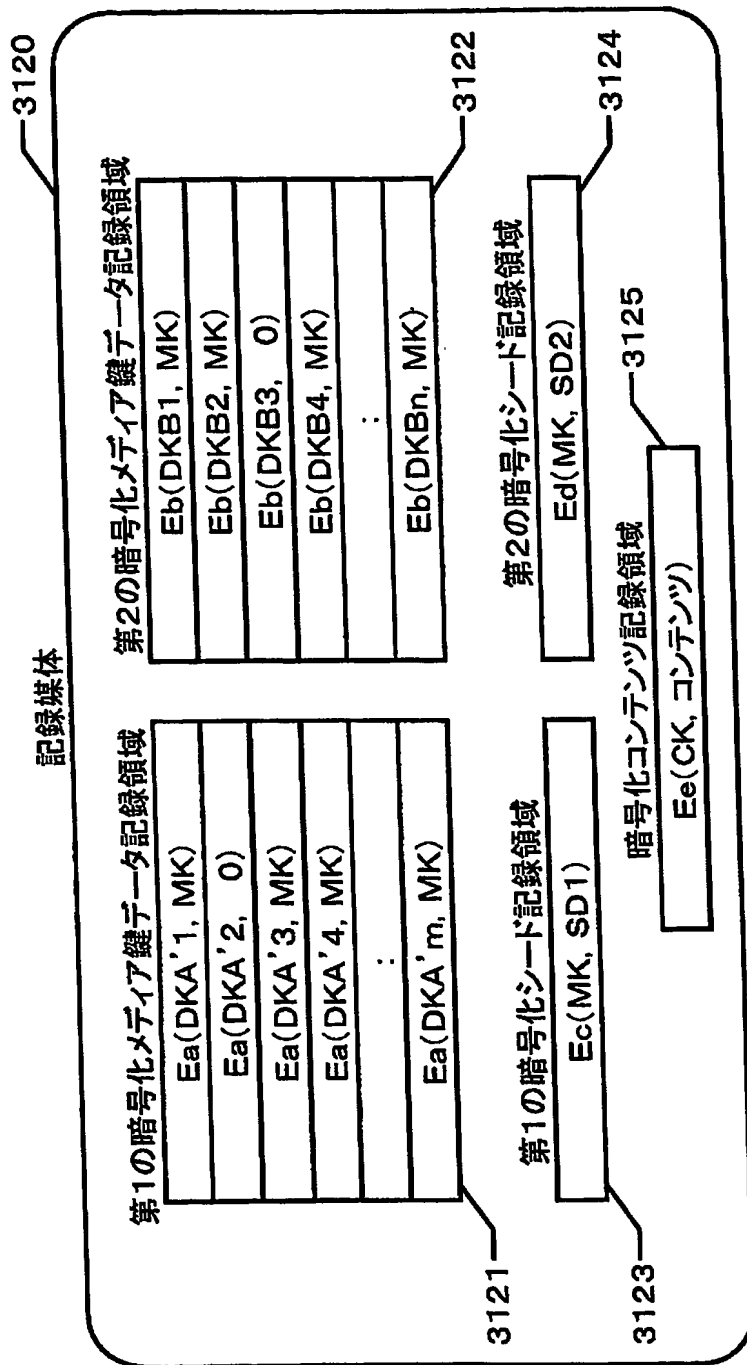
【図 34】

本発明の実施の形態6における記録媒体に記録するデータの具体例



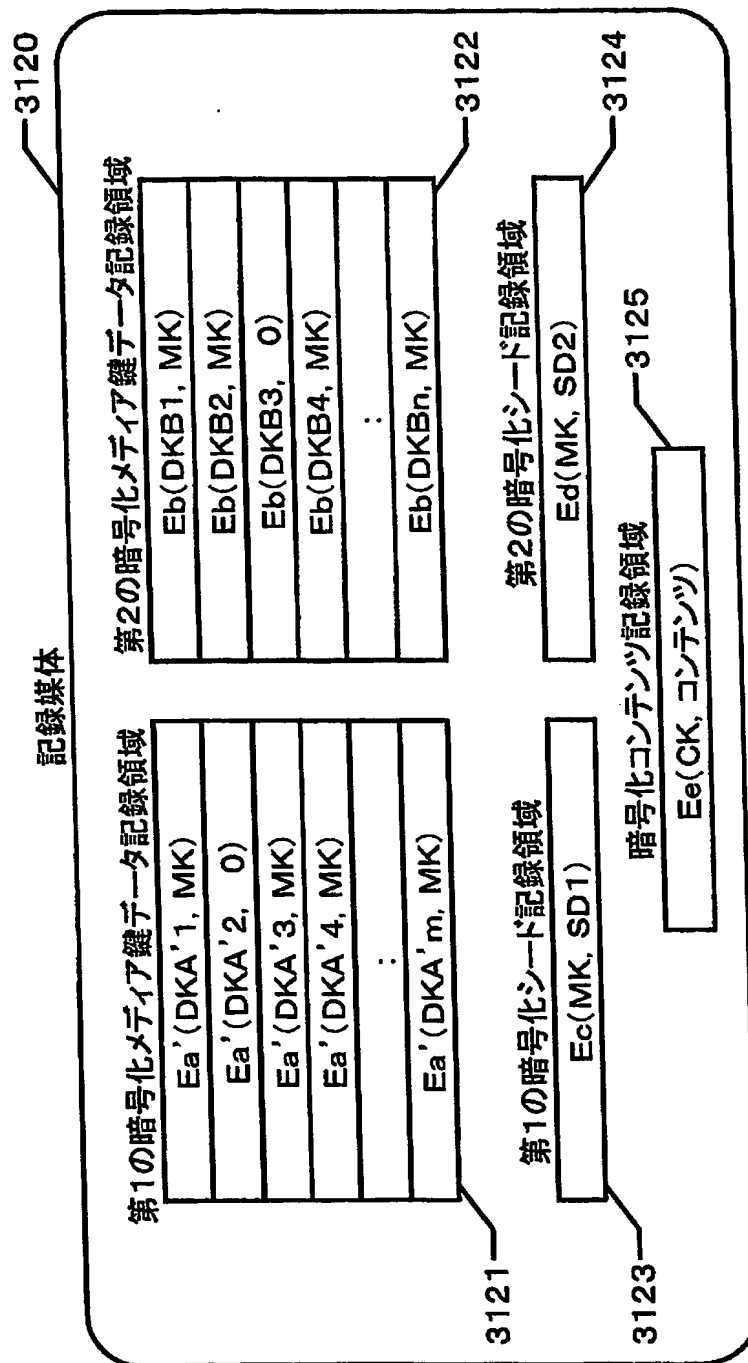
【図 35】

本発明の実施の形態6におけるシステム更新の具体例1



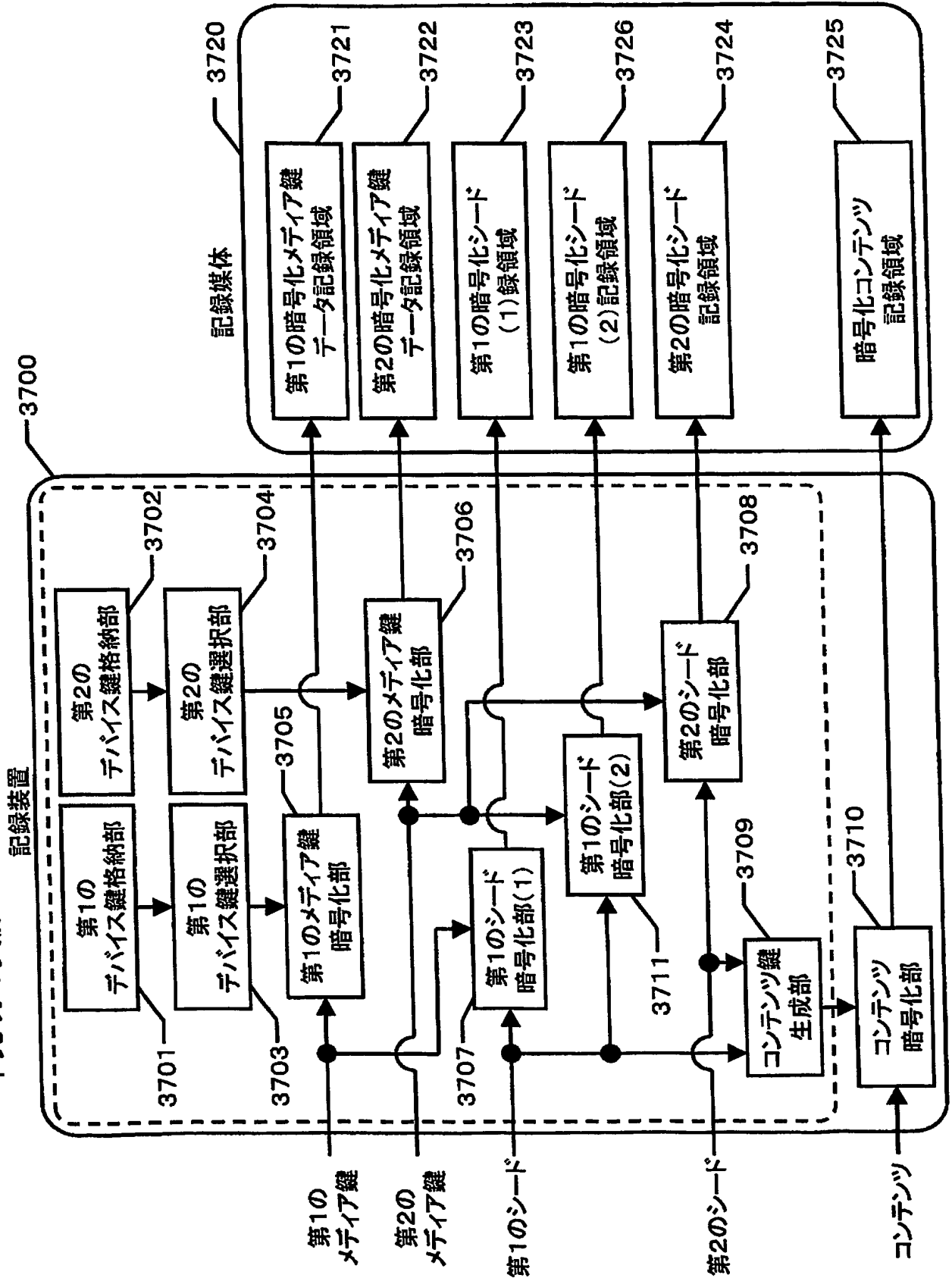
【図 36】

本発明の実施の形態6におけるシステム更新の具体例2



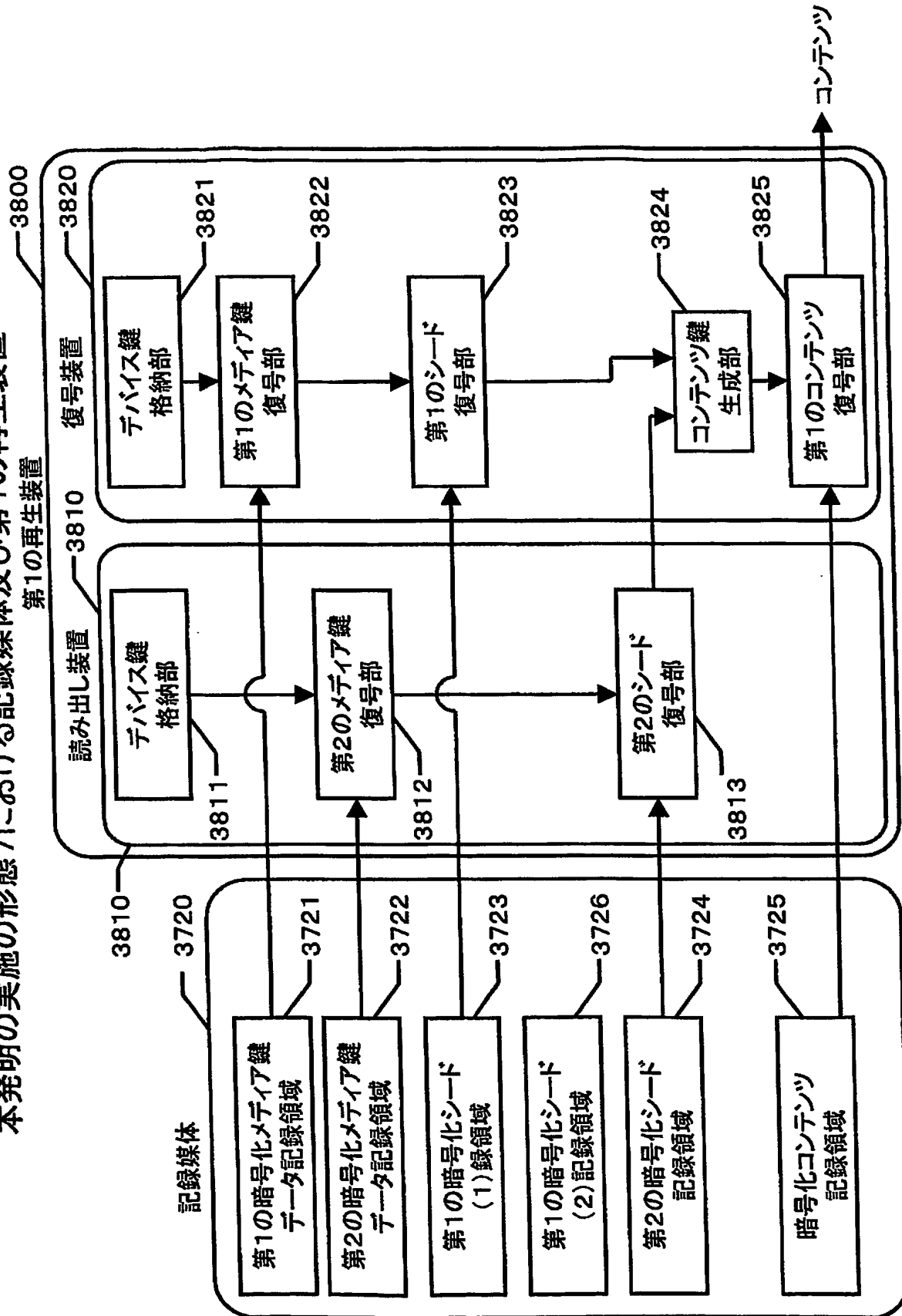
【図37】

本発明の実施の形態7における記録装置及び記録媒体



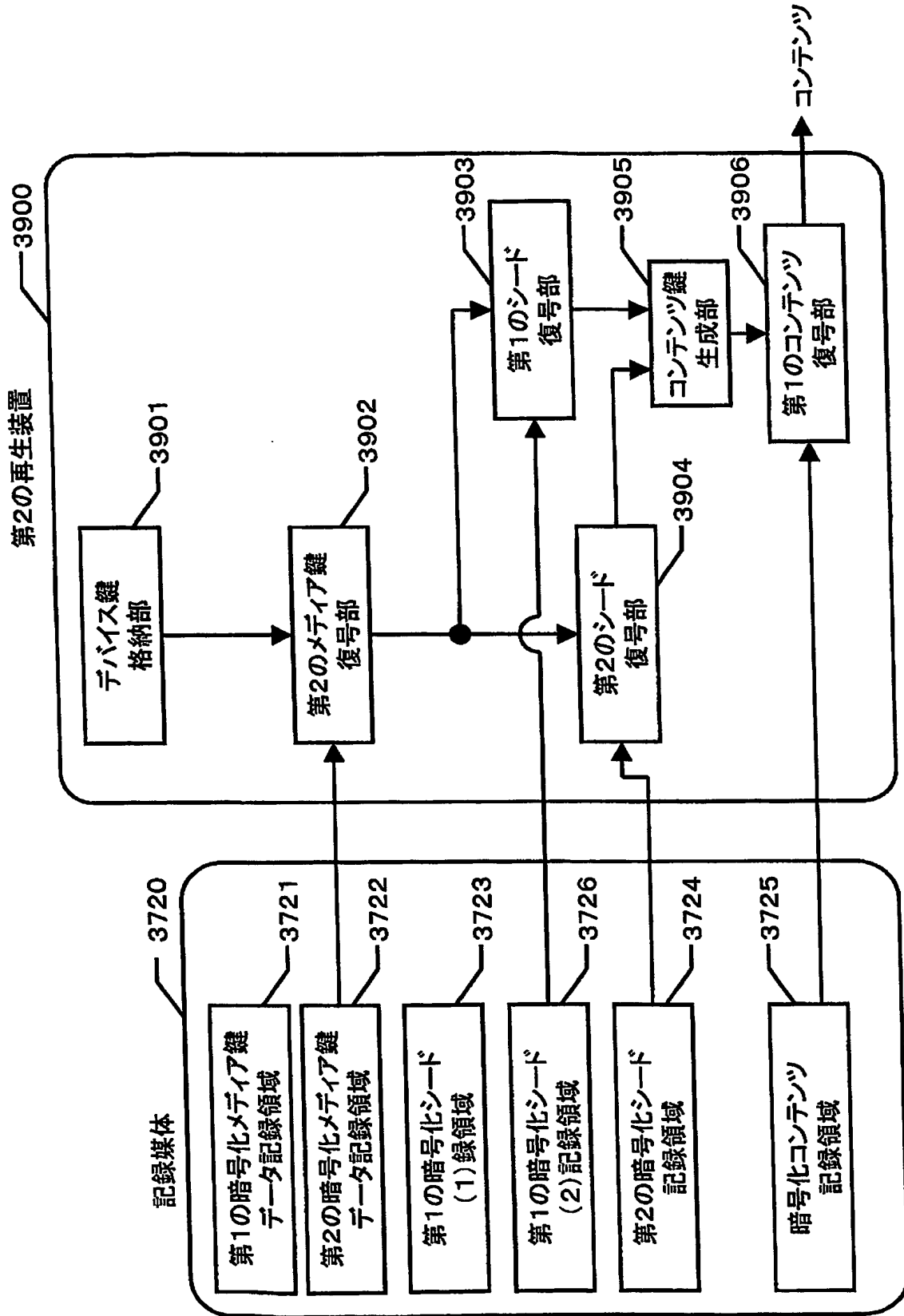
【図38】

本発明の実施の形態7における記録媒体及び第1の再生装置



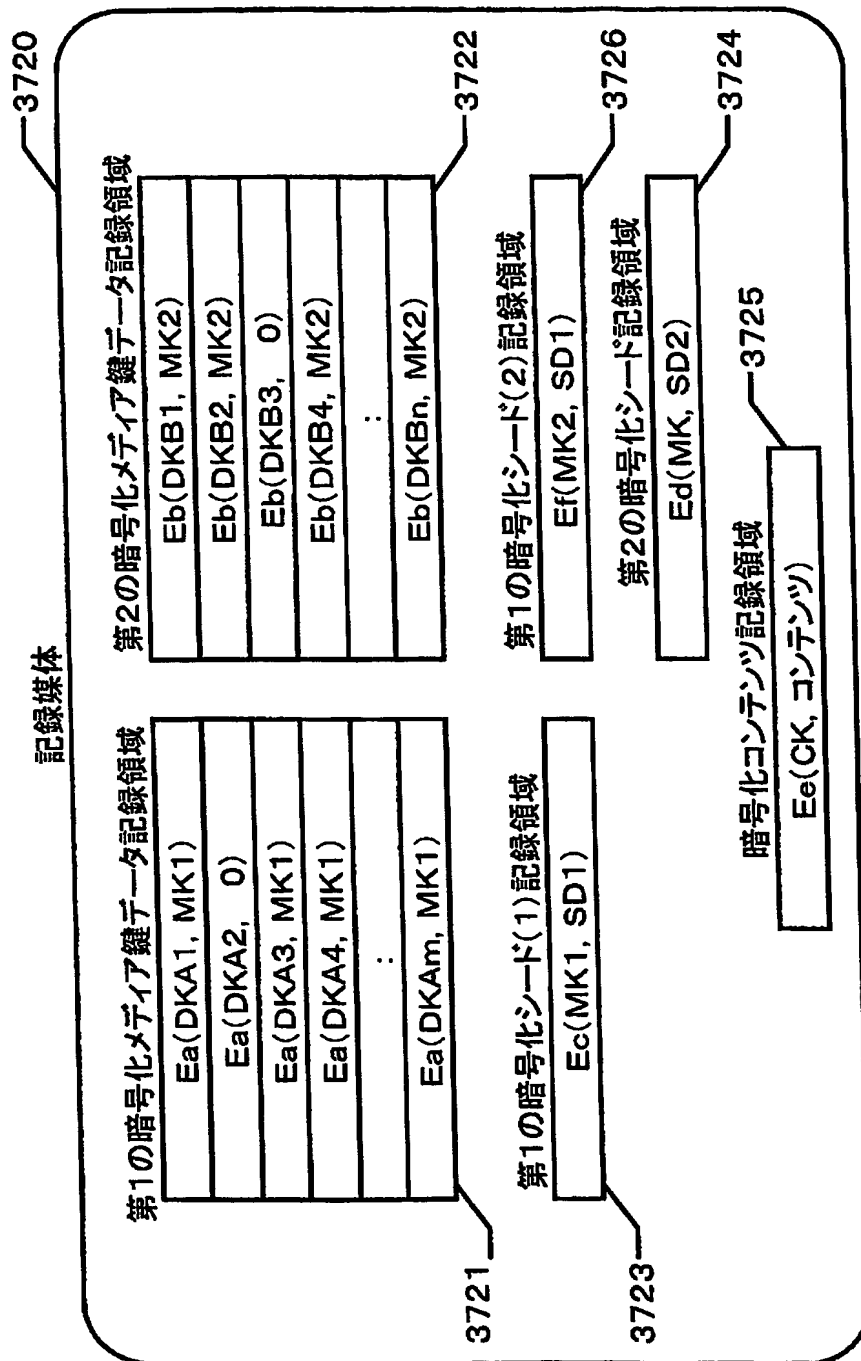
【図39】

本発明の実施の形態7における記録媒体及び第2の再生装置



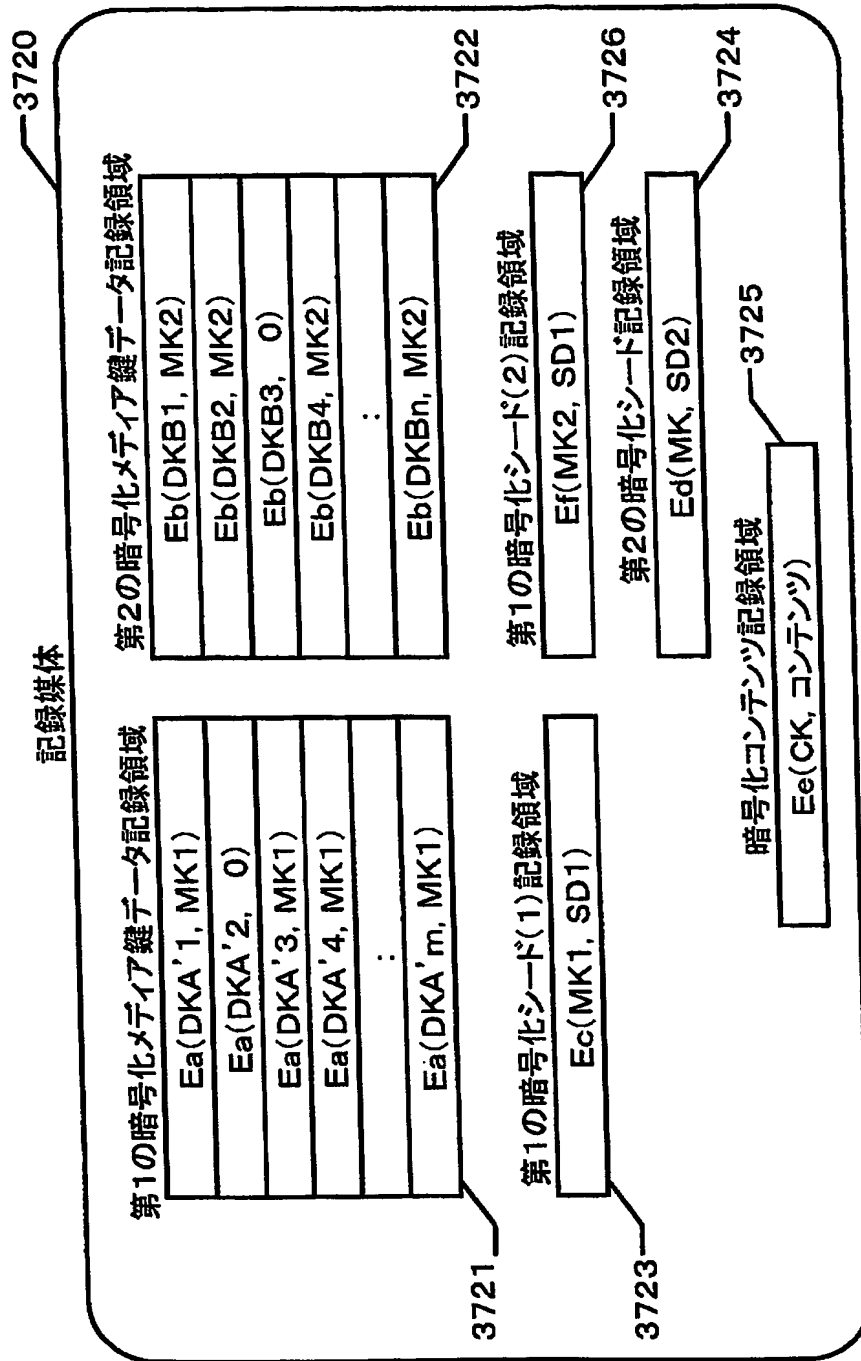
【図 40】

本発明の実施の形態7における記録媒体に記録するデータの具体例



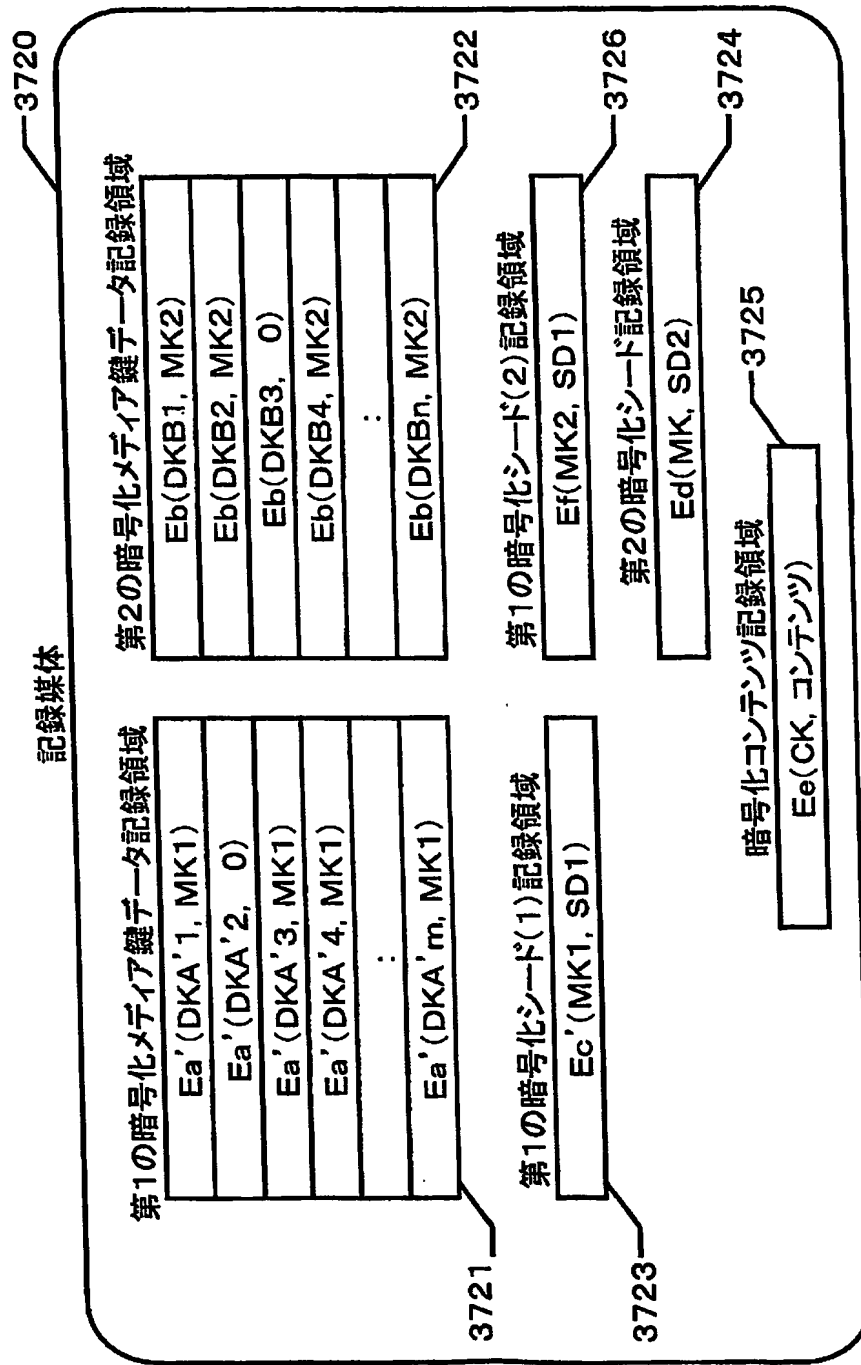
【図41】

本発明の実施の形態7におけるシステム更新の具体例1



【図42】

本発明の実施の形態7におけるシステム更新の具体例2



【書類名】 要約書**【要約】**

【課題】 装置内に設けるメモリのサイズを小さくでき、かつ、あるカテゴリの装置が不正に解析されてアルゴリズムや多数の鍵が暴露された場合でも、他のカテゴリの装置に変更を加えることなくシステム全体の無効化機能を維持することのできる著作権保護システムを提供する。

【解決手段】 装置は複数のカテゴリに分類されており、メディア鍵と各カテゴリに属する装置が保有するデバイス鍵データとから各カテゴリの特定の装置が保有するデバイス鍵を無効化するための無効化データを各カテゴリに対してそれぞれ生成し、記録媒体に記録する。

【選択図】 図 1

特願 2 0 0 3 - 2 8 6 6 5 7

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社

**This Page is Inserted by IFW Indexing and Scanning
Operations and is not part of the Official Record**

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☒ FADED TEXT OR DRAWING
- ☒ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☒ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☒ GRAY SCALE DOCUMENTS
- ☒ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.

As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.